

Elliptic curves related to cyclic cubic extensions

Rintaro Kozuma

Abstract. The aim of this paper is to study certain family of elliptic curves $\{\mathcal{X}_H\}_H$ defined over a number field F arising from hyperplane sections of some cubic surface \mathcal{X}/F associated to a cyclic cubic extension K/F . We show that each \mathcal{X}_H admits a 3-isogeny ϕ over F and the dual Selmer group $S^{(\phi)}(\widehat{\mathcal{X}_H}/F)$ is bounded by a kind of unit/class groups attached to K/F . This is proven via certain rational function on the elliptic curve \mathcal{X}_H with nice property. We also prove that the Shafarevich-Tate group $\text{III}(\widehat{\mathcal{X}_H}/\mathbb{Q})[\widehat{\phi}]$ coincides with a class group of K as a special case.

1. Introduction

The principal objects we are going to investigate are defined as follows. Let K/F be a cyclic cubic extension over a number field F with Galois group $G = \langle \sigma \rangle \simeq \mathbb{Z}/3\mathbb{Z}$, and let $\{1, \alpha_1, \alpha_2\}$ be a F -basis of K . Define a projective variety \mathcal{X} in the projective space \mathbb{P}^3 associated to the extension K/F with the F -basis $\{1, \alpha_1, \alpha_2\}$ of K by the homogeneous polynomial

$$(1.1) \quad f(x, y, z, w) := (x + y\alpha_1 + z\alpha_2)(x + y\alpha_1^\sigma + z\alpha_2^\sigma)(x + y\alpha_1^{\sigma^2} + z\alpha_2^{\sigma^2}) - w^3$$

with coefficients in F , which is a singular cubic hypersurface and rational over K . The elliptic curves we consider are hyperplane sections $\{\mathcal{X} \cap H\}_H$ of \mathcal{X} where H/F varies through all hyperplanes in \mathbb{P}^3 satisfying $(\mathcal{X} \cap H)(F) \neq \emptyset$. We shall simply denote by \mathcal{X}_H the section $\mathcal{X} \cap H$. For such a cubic curve \mathcal{X}_H/F we can prove (in Lemma 2.3) that

$$\begin{cases} \mathcal{X}_H/F \text{ is birationally equivalent over } F \text{ to } \mathbb{P}^1 \text{ if } H/F \text{ is tangent to } \mathcal{X}, \\ \mathcal{X}_H/F \text{ is an elliptic curve if } H/F \text{ is not tangent to } \mathcal{X}, \end{cases}$$

and it also turns out (in Proposition 2.2) that there is a hyperplane H_0/F on which the point $\mathcal{O} := [1, 0, 0, 1] \in \mathcal{X}(F)$ lies such that the cubic curve \mathcal{X}_H is isomorphic over F to \mathcal{X}_{H_0} . Therefore we may assume $\mathcal{O} \in H$ and fix \mathcal{O} as a base point on \mathcal{X}_H without loss of generality, namely the defining equation of H has the form $a(x-w) + by + cz = 0$ with $[a, b, c] \in \mathbb{P}^2(\mathfrak{O}_F)$ where \mathfrak{O}_F is the ring of integers of F .

Under the situation as above, our interest is the arithmetic nature of the elliptic curves $\{\mathcal{X}_H\}_H$ and how that relates to the arithmetic of the cyclic cubic extension K/F . Main results are stated as follows.

Theorem 1.1. *For any cyclic cubic extension K/F with a fixed F -basis $\{1, \alpha_1, \alpha_2\}$ of K and the Galois group $\text{Gal}(K/F) = \langle \sigma \rangle$, let $\mathcal{X} \subset \mathbb{P}^3$ be a cubic hypersurface over F defined by the polynomial (1.1). For a hyperplane $H : a(x - w) + by + cz = 0$ in \mathbb{P}^3 with coefficients $[a, b, c] \in \mathbb{P}^2(\mathfrak{O}_F)$ which is not tangent to \mathcal{X} , there is an isomorphism $\vartheta : \mathcal{X}_H \xrightarrow{\sim} \mathcal{W}(\mathcal{X}_H)$ over F mapping \mathcal{O} to $[0, 1, 0]$ with an elliptic curve $\mathcal{W}(\mathcal{X}_H) \subset \mathbb{P}^2$ over F given by the Weierstrass form*

$$(1.2) \quad y^2 + a\delta(\mathcal{X})xy - N_{K/F}(\gamma(\mathcal{X}_H))y = x^3$$

where $N_{K/F} : K^* \rightarrow F^*$ is the norm map and the constants $\delta(\mathcal{X}) \in F^*$, $\gamma(\mathcal{X}_H) \in K^*$ are defined by determinants

$$\delta(\mathcal{X}) = \begin{vmatrix} 1 & \alpha_1 & \alpha_2 \\ 1 & \alpha_1^\sigma & \alpha_2^\sigma \\ 1 & \alpha_1^{\sigma^2} & \alpha_2^{\sigma^2} \end{vmatrix}, \quad \gamma(\mathcal{X}_H) = \begin{vmatrix} 1 & \alpha_1 & \alpha_2 \\ 1 & \alpha_1^\sigma & \alpha_2^\sigma \\ a & b & c \end{vmatrix}.$$

Note that the isomorphism class of $\mathcal{W}(\mathcal{X}_H)$ is independent of the choice of the coordinate $(a, b, c) \in \mathbb{A}^3(\mathfrak{O}_F)$ and the generator σ of $\text{Gal}(K/F)$.

We retain the notation, and assume H is not tangent to \mathcal{X} . By the above theorem, there is the F -rational 3-torsion point $(0, 0)$ on $\mathcal{W}(\mathcal{X}_H)$, thus the elliptic curve \mathcal{X}_H/F always admits a 3-isogeny $\phi : \mathcal{X}_H \rightarrow \widehat{\mathcal{X}_H}$ defined over F where $\widehat{\mathcal{X}_H}/F$ stands for the dual elliptic curve $\mathcal{X}_H/\langle \vartheta^{-1}(0, 0) \rangle$. Let $\widehat{\phi}$ denote its dual isogeny. For any set S of finite primes of F , we denote by $\mathfrak{O}_{L,S}^*$, $\text{Cl}_{L,S}$ the group of S -units and the S -ideal class group of a finite extension L/F respectively (The precise definition will be given in §5). We make the general notation:

- $\overline{\Omega}$: an equivalence class represented by Ω , or an algebraic closure of Ω .
- $\langle \varepsilon \rangle$: a group generated by an element ε .
- $\Gamma[\varphi]$: the kernel of a homomorphism $\varphi : \Gamma \rightarrow \Gamma'$.
- $\nu_{\mathfrak{p}}$: the \mathfrak{p} -adic normalized valuation of a local field $L_{\mathfrak{p}}$. (i.e. $\nu_{\mathfrak{p}}(L_{\mathfrak{p}}) = \mathbb{Z}$)
- $\mu_3(L)$: the group of all cube roots of unity in a field L .

As for the Selmer groups $S^{(\widehat{\phi})}(\widehat{\mathcal{X}_H}/F)$, $S^{(\phi)}(\mathcal{X}_H/\mathbb{Q})$, we have the following results.

Theorem 1.2 (Partial result of Theorem 5.2).

$$\dim_{\mathbb{F}_3} S^{(\widehat{\phi})}(\widehat{\mathcal{X}_H}/F) \leq \dim_{\mathbb{F}_3} {}_N\mathfrak{U}_{K,S'} \oplus \mu_3(F) + \dim_{\mathbb{F}_3} {}_N\text{Cl}_{K,S'}^G[3] - \dim_{\mathbb{F}_3} \frac{{}_N\mathfrak{U}_{K,S'} \cap \mathfrak{O}_{F,S'}^*}{{}_N\mathfrak{U}_{K,S'}}$$

where ${}_N\mathfrak{U}_{K,S'}$, ${}_N\text{Cl}_{K,S'}[3]$, $K_{S'}$ are subgroups of $\mathfrak{O}_{K,S'}^*/\mathfrak{O}_{K,S'}^{*3}$, $\text{Cl}_{K,S'}[3]$, K^* respectively, which are defined in §5. The set S' is a subset of all finite primes \mathcal{P}_F of F , defined by

$$S' := \left\{ \mathfrak{p} \in \mathcal{P}_F \mid \begin{array}{l} \mathfrak{p} \text{ splits completely in } K \text{ and } \\ \text{or } 3\nu_{\mathfrak{p}}(a\delta(\mathcal{X})) < \nu_{\mathfrak{p}}(N_{K/F}(\gamma(\mathcal{X}_H))) \\ \text{or } \nu_{\mathfrak{p}}(N_{K/F}(\gamma(\mathcal{X}_H))) \not\equiv 0 \pmod{3} \end{array} \right\}.$$

Furthermore if $\text{Cl}_{K,S'}$ is G -invariant then $\mathcal{X}_H(F)/\widehat{\phi}(\widehat{\mathcal{X}_H}(F)) \hookrightarrow {}_N\mathfrak{U}_{K,S'} \oplus \mu_3(F)$.

As a special case, we can state more precise result.

Theorem 1.3. *For a cyclic cubic field K/\mathbb{Q} , let $\{1, \alpha, \alpha^2\}$ be a \mathbb{Q} -basis of K that \mathcal{X} is defined by the polynomial (1.1) with. Here $\alpha \in K$ denotes a root of the generic polynomial $\mathfrak{g}(x; t)$ in §8 for some $t \in \mathbb{Q}$. Let H be the hyperplane $z = 0$. Assume $t \in \mathbb{Z}$, $\pm N_{K/F}(\alpha - \alpha^\sigma) = t^2 + 3t + 9 \notin \mathbb{Q}_3^{*3}$. Then $S' = \emptyset$ and*

$$\dim_{\mathbb{F}_3} S^{(\phi)}(\mathcal{X}_H/\mathbb{Q}) = \dim_{\mathbb{F}_3} S^{(\widehat{\phi})}(\widehat{\mathcal{X}_H}/\mathbb{Q}) = 1 + \dim_{\mathbb{F}_3} {}_N\mathrm{Cl}_K^G[3],$$

$$1 \leq \mathrm{rank}_{\mathbb{Z}} \mathcal{X}_H(\mathbb{Q}) \leq 1 + 2 \dim_{\mathbb{F}_3} {}_N\mathrm{Cl}_K^G[3].$$

Furthermore, we also assume that Cl_K is G -invariant. Then

$$\begin{aligned} \mathcal{X}_H(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{X}_H}(\mathbb{Q})) &\simeq {}_N\mathfrak{U}_K \simeq \mathbb{Z}/3\mathbb{Z}, \\ \mathrm{III}(\widehat{\mathcal{X}_H}/\mathbb{Q})[\widehat{\phi}] &\simeq {}_N\mathrm{Cl}_K[3]. \end{aligned}$$

Here III stands for the Shafarevich-Tate group.

The present paper is organized as follows. First, we will give basic properties of the cubic surface \mathcal{X}/F and the family of its hyperplane sections in §2. Using these properties and a generic polynomial for cyclic cubic extensions (in §8), we obtain a Weierstrass form of the cubic curve \mathcal{X}_H in §3. We will discuss, in §4, descent theory for \mathcal{X}_H via 3-isogeny, and give some relation between Selmer groups and unit/class groups in §5. We also refer corollaries and remarks of the above theorems to the corresponding sections.

2. First properties of \mathcal{X} and its hyperplane sections

Fix a cyclic cubic extension K over a number field F with Galois group $G = \langle \sigma \rangle \simeq \mathbb{Z}/3\mathbb{Z}$, once and for all. For any F -basis $\{1, \alpha_1, \alpha_2\}$ of K , let \mathcal{X}/F be a cubic surface in \mathbb{P}^3 defined by the polynomial (1.1). It is easy to verify that the cubic surface \mathcal{X}/F has three singular points on the hyperplane $w = 0$, and is birationally equivalent over K to the projective plane \mathbb{P}^2 .

Let $\mathcal{L}(\mathcal{X})$ be a set of all those hyperplanes $\{H\}$ defined over F in \mathbb{P}^3 which satisfy $\mathcal{X}_H(F) \neq \emptyset$. From the definition, we observe the following.

Lemma 2.1. *The family $\mathcal{L}(\mathcal{X})$ is invariant under the change of F -basis of K .*

Proof. Since any basis transformation for a vector space is linear and defined over a ground field, the lemma follows immediately. \square

From now on, we choose any F -basis of K and fix it without loss of generality. From the definition of \mathcal{X} , the affine piece $\mathcal{X}_{w \neq 0} := \mathcal{X} \cap \{w \neq 0\}$ of the surface \mathcal{X} has a structure of linear algebraic groups by a natural correspondence between the group of F -rational points $\mathcal{X}_{w \neq 0}(F) = \mathcal{X}(F)$ and the kernel of the norm map:

$$\begin{aligned} \mathcal{X}_{w \neq 0}(F) &\xrightarrow{\sim} \mathrm{Ker} [K^* \xrightarrow{N_{K/F}} F^*] \\ [x, y, z, 1] &\longmapsto x + y\alpha_1 + z\alpha_2. \end{aligned}$$

The rational function $x + y\alpha_1 + z\alpha_2$ on $\mathcal{X}_{w \neq 0}$ also induces an isomorphism

$$\mathcal{X}_{w \neq 0}(\mathfrak{O}_F) \xrightarrow{\sim} \mathrm{Ker} [\mathfrak{O}_K^* \xrightarrow{N_{K/F}} \mathfrak{O}_F^*]$$

if the set $\{1, \alpha_1, \alpha_2\}$ forms an \mathfrak{O}_F -basis of \mathfrak{O}_K . For instance this holds for the case that the class number of the ground field F is equal to 1. Particularly in the case $F = \mathbb{Q}$, we have $\mathcal{X}(\mathbb{Z}) \simeq \mathfrak{O}_K^*/\{\pm 1\}$ for an integral basis of K . Thus, in this case, we can regard the group of units \mathfrak{O}_K^* as the group of \mathbb{Z} -valued points on the variety \mathcal{X} . This identification is one of the reason why we adopt the algebraic variety \mathcal{X} in view of the analogy between Mordell-Weil groups of elliptic curves and groups of units. Accordingly it might be of some interest to deduce the arithmetic of the elliptic curves $\{\mathcal{X}_H\}_H$ from the cyclic cubic extension K/F , and that is exactly what we propose to carry out in the present paper. Note that the above isomorphism can be naturally generalized to the group $\mathcal{X}(\mathfrak{O}_{F,S})$ where $\mathfrak{O}_{F,S}$ is a ring of S -integers of F . We will see a considerable aspect of the function $x + y\alpha_1 + z\alpha_2$ in §6, which is the most essential part of the paper to obtain an arithmetic relation between the section \mathcal{X}_H/F and the ambient variety \mathcal{X}/F reflecting the cyclic cubic extension K/F .

For any point $P \in \mathcal{X}_{w \neq 0}(F)$, the left translation $\mathcal{X}_{w \neq 0}(F) \rightarrow \mathcal{X}_{w \neq 0}(F); Q \mapsto P \cdot Q$ causes the faithful regular representation ρ of degree 3 and the canonical enlargement $\tilde{\rho}$

$$\begin{aligned} \tilde{\rho} : \mathcal{X}_{w \neq 0}(F) &\xrightarrow{\rho} \mathrm{GL}_3(F) \longrightarrow \mathrm{PGL}_4(F) \\ \rho(P) &\longmapsto \begin{pmatrix} \rho(P) & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

The representation $\tilde{\rho}$ induces a linear action of the group $\mathcal{X}_{w \neq 0}(F)$ on the set $\mathcal{X}(\overline{F})$

$$\begin{aligned} \mathcal{X}_{w \neq 0}(F) \times \mathcal{X}(\overline{F}) &\longrightarrow \mathcal{X}(\overline{F}) \\ (P, [x, y, z, w]) &\longmapsto [x, y, z, w] \cdot \tilde{\rho}(P). \end{aligned}$$

Note that $\mathcal{X}(\overline{F})$ is only a set, not a group. Thus each element in $\mathcal{X}_{w \neq 0}(F)$ gives an isomorphism on \mathcal{X} , and hence we obtain an action of $\mathcal{X}_{w \neq 0}(F)$ on the family $\mathcal{L}(\mathcal{X})$ defined by $P \cdot \mathcal{X}_H := \mathcal{X}_{\tilde{\rho}(P)(H)}$. This action makes matter somewhat simple as follows.

Proposition 2.2. *For arbitrary hyperplane $H \in \mathcal{L}(\mathcal{X})$, there is a hyperplane $H_0 \in \mathcal{L}(\mathcal{X})$ on which the point \mathcal{O} lies so as to be $\mathcal{X}_H \simeq \mathcal{X}_{H_0}$ over F .*

Proof. This is almost clear. For any $H \in \mathcal{L}(\mathcal{X})$ with a F -rational point $P \in \mathcal{X}_H(F) \subset \mathcal{X}_{w \neq 0}(F)$, the hyperplane $H_0 := \tilde{\rho}(P^{-1})(H)$ satisfies the property of the statement. \square

By Proposition 2.2, the study of the cubic curves $\{\mathcal{X}_H\}_H$ where H/F varies through $\mathcal{L}(\mathcal{X})$ is reduced to the family of curves \mathcal{X}_H which possess the point $\mathcal{O} \in H$. We shall denote by $\mathcal{L}(\mathcal{O})$ the set of all hyperplanes in \mathbb{P}^3 defined over F on which the point \mathcal{O} lies. The following lemma gives a criterion for \mathcal{X}_H being an elliptic curve.

Lemma 2.3. *The following conditions are equivalent for any $H/F \in \mathcal{L}(\mathcal{X})$.*

- ◇ *The cubic curve \mathcal{X}_H/F is singular.*
- ◇ *The hyperplane H/F is tangent to the surface \mathcal{X}/F .*

Under these conditions, the cubic curve \mathcal{X}_H/F is birational over F to the projective line.

Proof. Since a linear transformation sends a tangent plane to a tangent plane, it suffices to prove the lemma for any hyperplane $H \in \mathcal{L}(\mathcal{O})$. We first show that the points on $\mathcal{X}_H \cap \{w = 0\}$ are non-singular. Let $\iota(x, y, z, w)$ be the rational function $x + y\alpha_1 + z\alpha_2 \in K[\mathcal{X}_H]$. The defining equation of \mathcal{X}_H is written by

$$f_H(x, y, z, w) := \iota(x, y, z, w) \iota^\sigma(x, y, z, w) \iota^{\sigma^2}(x, y, z, w) - w^3 \bmod a(x-w) + by + cz.$$

It is easily verified that the unique zero of the function ι on \mathcal{X}_H is

$$(2.1) \quad \mathcal{O}' := [c\alpha_1 - b\alpha_2, a\alpha_2 - c, -a\alpha_1 + b, 0]$$

and hence the set $\mathcal{X}_H \cap \{w = 0\}$ consists of three points $\{\mathcal{O}', \mathcal{O}'^\sigma, \mathcal{O}'^{\sigma^2}\}$. Thus we have

$$\frac{\partial f_H}{\partial x}(\mathcal{O}') = \left(1 + \frac{\partial y}{\partial x}(\mathcal{O}') \alpha_1 + \frac{\partial z}{\partial x}(\mathcal{O}') \alpha_2\right) \iota^\sigma(\mathcal{O}') \iota^{\sigma^2}(\mathcal{O}').$$

Here the partial derivatives are given by

$$\frac{\partial y}{\partial x}(\mathcal{O}') = \begin{cases} -\frac{a}{b} & \text{if } b \neq 0 \\ 0 & \text{if } b = 0, \end{cases} \quad \frac{\partial z}{\partial x}(\mathcal{O}') = \begin{cases} -\frac{a}{c} & \text{if } c \neq 0 \\ 0 & \text{if } c = 0. \end{cases}$$

Using this yields the non-singularity of the point \mathcal{O}' on \mathcal{X}_H . Acting the Galois group $\text{Gal}(K/F) = \langle \sigma \rangle$ yields non-singularity of the points \mathcal{O}'^σ and \mathcal{O}'^{σ^2} at once.

Now we consider the affine piece $\mathcal{X}_H \cap \{w \neq 0\}$. Since the Jacobian matrix for \mathcal{X}_H at a point P may be written by

$$J_P = \begin{pmatrix} \frac{\partial f}{\partial x}(P) & \frac{\partial f}{\partial y}(P) & \frac{\partial f}{\partial z}(P) \\ a & b & c \end{pmatrix},$$

the point $P \in \mathcal{X}_H$ is singular if and only if there is some constant $\lambda \in F(P)^*$ satisfying

$$(a, b, c) = \lambda \left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P), \frac{\partial f}{\partial z}(P) \right).$$

This implies the first equivalence. \square

Recall we have fixed the point \mathcal{O} as a base point of the cubic curve \mathcal{X}_H . In the proof of Lemma 2.3, we observe

$$\mathcal{X}_H \cap \{w = 0\} = \{\mathcal{O}', \mathcal{O}'^\sigma, \mathcal{O}'^{\sigma^2}\} \text{ where } \mathcal{O}' \text{ is the point (2.1).}$$

We end this section with the following fact.

Lemma 2.4. *Assume $H \in \mathcal{L}(\mathcal{O})$ is not tangent to \mathcal{X} . Then $3\mathcal{O}' \in \mathcal{X}_H(F)$. Moreover $\mathcal{O}'^\sigma - \mathcal{O}' = -(\mathcal{O}'^{\sigma^2} - \mathcal{O}') \in \mathcal{X}_H(F)[3] \setminus \{\mathcal{O}\}$.*

Proof. This follows from direct calculation by the “chord and tangent processes”. It can be verified that the tangent line at \mathcal{O}' meets \mathcal{X}_H again at \mathcal{O}' , namely the intersection is an inflection point. This implies the first statement of the lemma. As for the latter, the points $\mathcal{O}', \mathcal{O}'^\sigma, \mathcal{O}'^{\sigma^2}$ are collinear and the tangent line at \mathcal{O} meets \mathcal{X}_H again at $3\mathcal{O}'$ by the former proof. It thus turns out that $\mathcal{O}' + \mathcal{O}'^\sigma + \mathcal{O}'^{\sigma^2} = 3\mathcal{O}'$, which yields the required result. \square

3. Weierstrass form of the cubic curve \mathcal{X}_H over F

Proposition 2.2 in the previous section allows us to calculate a Weierstrass form of the cubic curve \mathcal{X}_H systematically. As the F -rational point \mathcal{O} on \mathcal{X}_H is given explicitly, the defining equation of \mathcal{X}_H/F can be transformed into Weierstrass form. For instance, see Cassels's book [5] as for this method. The proof of Theorem 1.1 sits in the end of this section. The corollaries below are immediate consequences read off from the Weierstrass form (1.2).

Corollary 3.1 (of Theorem 1.1). *The discriminant of the Weierstrass form (1.2) is*

$$\Delta(\mathcal{X}_H) = -N_{K/F}(\gamma(\mathcal{X}_H))^3 (a^3\delta(\mathcal{X})^3 + 3^3N_{K/F}(\gamma(\mathcal{X}_H))) .$$

Assume $H \in \mathcal{L}(\mathcal{O})$ is not tangent to \mathcal{X} . Then the j -invariant is

$$j(\mathcal{X}_H) = -\frac{a^3\delta(\mathcal{X})^3 (a^3\delta(\mathcal{X})^3 + 24N_{K/F}(\gamma(\mathcal{X}_H)))^3}{N_{K/F}(\gamma(\mathcal{X}_H))^3 (a^3\delta(\mathcal{X})^3 + 3^3N_{K/F}(\gamma(\mathcal{X}_H)))} .$$

Epecially the family $\{\mathcal{X}_H/F\}_{H \in \mathcal{L}(\mathcal{O})}$ contains infinitely many isomorphism class of elliptic curves.

Proof. A direct calculation. For example, see [11]. □

Corollary 3.2 (of Theorem 1.1). *Assume $H \in \mathcal{L}(\mathcal{O})$ is not tangent to \mathcal{X} . Then $(0, 0) = -(0, N_{K/F}(\gamma(\mathcal{X}_H))) \in \mathcal{W}(\mathcal{X}_H)(F)[3] \setminus \{[0, 1, 0]\}$.*

Proof. Since these points are inflection points, the statement follows. □

Remark 3.3. By Corollary 3.2, there is a dual elliptic curve $\widehat{\mathcal{X}_H}$ defined over F which is isomorphic to $\mathcal{W}(\mathcal{X}_H)/\langle(0, 0)\rangle$ given by the Weierstrass form (For example, see [9])

$$y^2 + a\delta(\mathcal{X})xy + 3^2N_{K/F}(\gamma(\mathcal{X}_H))y = x^3 + N_{K/F}(\gamma(\mathcal{X}_H)) (a^3\delta(\mathcal{X})^3 - 3^3N_{K/F}(\gamma(\mathcal{X}_H))) .$$

Remark 3.4. The family $\{\mathcal{X}_H/F\}_{H \in \mathcal{L}(\mathcal{O})}$ is independent of the choice of F -basis of K , but each curve \mathcal{X}_H/F depends on.

Remark 3.5. For arbitrary $(a, b, c) \in \mathbb{A}^3(F)$, define $\gamma(a, b, c)$ to be the discriminant of the same matrix as $\gamma(\mathcal{X}_H)$ in Theorem 1.1. Then, as a matter of fact, the quantity $N_{K/F}(\gamma(a, b, c))$ is $\mathcal{X}_{w \neq 0}(F)$ -invariant, namely $N_{K/F}(\gamma((a, b, c)\rho(P))) = N_{K/F}(\gamma(a, b, c))$ for arbitrary $P \in \mathcal{X}_{w \neq 0}(F)$. Especially we have $N_{K/F}(\gamma(\mathcal{X}_H)) = N_{K/F}(\gamma(\mathcal{X}_{\tilde{\rho}(P)(H)}))$ for any $P \in \mathcal{X}_{w \neq 0}(F)$ by taking suitable coefficients of hyperplanes as follows. Let $[a, b, c] \in \mathbb{P}^2(\mathfrak{D}_F)$ be coefficients of any hyperplane $H/F \in \mathcal{L}(\mathcal{O})$. Take $(a', b', c') := (a, b, c)\rho(P)$ for arbitrary $P \in \mathcal{X}_{w \neq 0}(F)$. Then the hyperplane $H' := \tilde{\rho}(P)(H)$ has the defining equation $a'(x - x_0w) + b'(y - y_0w) + c'(z - z_0w) = 0$ where $(x_0, y_0, z_0) := (1, 0, 0)^t \rho(P)^{-1}$. Further if P lies on $\mathcal{X}_H(F)$ then one can observe that $a = a'$. This fact implies that for any $P \in \mathcal{X}_H(F)$ the section $\mathcal{X}_{H'}$ by the hyperplane $H' := \tilde{\rho}(P^{-1})(H) \in \mathcal{L}(\mathcal{O})$ has the Weierstrass form (1.2). In connection with Proposition 2.2, it thus turns out that the Weierstrass form (1.2) of \mathcal{X}_H is invariant for the choice of a point on $\mathcal{X}_H(F)$.

From now on we shall show necessary lemmas for the proof of Theorem 1.1. First, we choose a generic polynomial for $C_3 \simeq \mathbb{Z}/3\mathbb{Z}$ -extension over F ,

$$(\mathfrak{g}(x) =) \mathfrak{g}(x; t) = x^3 + t x^2 - (t + 3)x + 1 \quad (t \in F, \delta(\mathfrak{g}) = t^2 + 3t + 9).$$

We recall basic properties of this polynomial in §8 briefly. By the property, for any cyclic cubic extension K/F , there is a constant $t \in F$ such that the roots of $\mathfrak{g}(x; t)$ generates K over F . Fix $t \in F$ for K/F and $\alpha \in K$ as one of the roots. Let \mathcal{X}^0/F be a cubic hypersurface in \mathbb{P}^3 associated to K/F with the F -basis $\{1, \alpha, \frac{1}{1-\alpha}\}$ of K defined by the same polynomial as (1.1).

For this \mathcal{X}^0/F and any hyperplane $H \in \mathcal{L}(\mathcal{O})$, we prove as follows that the curve \mathcal{X}_H^0 is birational over F to either the cubic curve $\mathcal{W}(\mathcal{X}_H^0)$ defined by the same Weierstrass form as (1.2) or \mathbb{P}^1 by dividing it into 3-cases according to embeddings of \mathcal{X}_H^0 into \mathbb{P}^2 as plane cubic curves.

Lemma 3.6. *Let $H : a(x - w) + by + cz = 0$ be a hyperplane in \mathbb{P}^3 defined over F . Assume $at + 3c \neq 0$. Then there is a birational map given by*

$$\begin{aligned} \theta : \mathcal{X}_H^0 &\xrightarrow{\sim} \mathcal{W}(\mathcal{X}_H^0); \\ [x, y, z, w] &\longmapsto [\theta_X, \theta_Y, \theta_Z], \\ [\theta_X^{(-1)}, \theta_Y^{(-1)}, \theta_Z^{(-1)}, \theta_W^{(-1)}] &\longleftarrow [x, y, z], \\ \begin{cases} \theta_X = u_0 u_1^2 \left(\frac{y-3c_0 w}{h_0(x, y, z, w)w} + \frac{3A^2\delta(\mathfrak{g})+c_7}{c_1} \right) w, \\ \theta_Y = u_0 u_1^3 \left(\frac{2}{3} g_3 \left[\frac{y-3c_0 w}{h_0(x, y, z, w)w} \right] h_0(x, y, z, w) + g_2 \left[\frac{y-3c_0 w}{h_0(x, y, z, w)w} \right] \right) w - \frac{a\delta(\mathfrak{g})\theta_X - N_{K/F}(\gamma(\mathcal{X}_H^0))w}{2}, \\ \theta_Z = w, \end{cases} \\ \begin{cases} \theta_X^{(-1)} = (1 + t(-A - B h_1(x, z) + h_1(x, z))) h_2(x, y, z)z + (1 + t c_0(1 - B))z, \\ \theta_Y^{(-1)} = 3(h_1(x, z) h_2(x, y, z) + c_0)z, \\ \theta_Z^{(-1)} = 3(-(A + B h_1(x, z)) h_2(x, y, z) - B c_0)z, \\ \theta_W^{(-1)} = z. \end{cases} \end{aligned}$$

Here the functions $h_0(x, y, z, w)$, $h_1(x, z)$, $h_2(x, y, z) \in F(x, y, z, w)$ are

$$\begin{aligned} h_0(x, y, z, w) &= 3\left(\frac{x}{w} - 1\right) - t\frac{y}{w} - t\frac{z}{w}, \quad h_1(x, z) = \frac{x}{u_0 u_1^2 z} - \frac{3A^2\delta(\mathfrak{g}) + c_7}{c_1}, \\ h_2(x, y, z) &= \frac{(y + 2^{-1}(a\delta(\mathfrak{g})x - N_{K/F}(\gamma(\mathcal{X}_H^0))z)) - g_2[h_1(x, z)]u_0 u_1^3 z}{2 g_3[h_1(x, z)]u_0 u_1^3 z}, \end{aligned}$$

and the functions $g_2[X]$, $g_3[X]$ are elements in the ring of polynomials $F[X]$ defined by

$$\begin{aligned} g_3[X] &= c_1\delta(\mathfrak{g})X^3 + 3c_2\delta(\mathfrak{g})X^2 + 3Ac_3\delta(\mathfrak{g})X + c_4, \\ g_2[X] &= 6(B^2 + B + 1)\delta(\mathfrak{g})X^2 + 3\frac{c_5}{c_1}\delta(\mathfrak{g})X + 3A\frac{c_6}{c_1}\delta(\mathfrak{g}) + 3, \end{aligned}$$

where $(A, B) = (\frac{a}{at+3c}, \frac{at+3b}{at+3c})$ and the other constants are as follows.

$$c_0 = \frac{3(B^2 + B + 1)}{c_1}, \quad u_0 = -12\delta(\mathfrak{g})c_1, \quad u_1 = \frac{at + 3c}{18},$$

$$\begin{aligned}
c_1 &= (B+2)^3 \mathfrak{g} \left(\frac{-B+1}{B+2} \right), \\
c_2 &= A (B^2(2t+3) + 2B(t+6) - t + 3) - (B^2 + B + 1), \\
c_3 &= A (B(2t+3) + t + 6) - 2B - 1, \\
c_4 &= (3A)^3 \mathfrak{g} \left(\frac{1-At}{3A} \right), \\
c_5 &= A (4B^4(2t+3) + B^3(16t+51) + 3B^2(7t+24) + B(13t+87) - 4t + 21) - 6(B^2 + B + 1)^2, \\
c_6 &= A (2B^3(2t+3) + 3B^2(2t+3) + 6B(2t+3) + 5t + 21) - 3((B+1)^3 + B^3), \\
c_7 &= A (B^2(2t+3) + 2B(t+6) - t + 3) - 2(B^2 + B + 1).
\end{aligned}$$

Proof. On account of technical reason, we first make the substitution

$$[x, y, z, w] \xrightarrow{i} [x, y, z, w] \cdot \begin{pmatrix} 3 & 0 & 0 & 0 \\ -t & 1 & 0 & 0 \\ -t & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

which maps the point \mathcal{O} to \mathcal{O} . The substitution i maps the hyperplane $H : a(x-w) + by + cz = 0$ to the hyperplane $i(H) : a(x-w) + (at+3b)y + (at+3c)z = 0$. We denote the polynomial $f \circ i^{-1}$ defining $i(\mathcal{X}^0)$ by ${}^i f$ where f denotes the polynomial defining \mathcal{X}^0 . From the assumption $at+3c \neq 0$, we have the cubic form ${}^i f_H(x, y, w) := {}^i f(x, y, -A(x-w) - By, w)$ which defines the plane cubic curve $i(\mathcal{X}_H^0) = i(\mathcal{X}^0) \cap i(H) \hookrightarrow \mathbb{P}^2$ isomorphic to \mathcal{X}_H^0 . We may regard a point $[x, y, w]$ on \mathbb{P}^2 as an affine point $(x/w, y/w) \in \mathbb{A}^2$ if $w \neq 0$. Then \mathcal{O} may be identified with $(1, 0)$.

The tangent at $(1, 0) \in i(\mathcal{X}_H^0)$ meets $i(\mathcal{X}_H^0)$ again at a F -rational point P , say. It is easily calculated that $P = (1, c_0) \in i(\mathcal{X}_H^0)$. Let $g_H(x, y) := {}^i f_H(x+1, y+c_0, 1)$. Using the method in Cassels's book [5], there is a birational map Θ over F from the cubic curve $i(\mathcal{X}_H^0)$ to a curve \mathcal{C} whose defining equation of the affine piece $\{w \neq 0\}$ is given by

$$y^2 = g_2[x]^2 - 4g_1[x]g_3[x]$$

where $g_d[x]$ denotes the homogeneous part of degree d of the polynomial $g_H(1, x)$. The map Θ is given by

$$\begin{aligned}
\Theta : i(\mathcal{X}_H^0) &\xrightarrow{\sim} \mathcal{C} \\
(x, y) &\longmapsto \left(\frac{y-c_0}{x-1}, 2g_3 \left[\frac{y-c_0}{x-1} \right] (x-1) + g_2 \left[\frac{y-c_0}{x-1} \right] \right), \\
\left(\frac{y-g_2[x]}{2g_3[x]} + 1, \frac{y-g_2[x]}{2g_3[x]}x + c_0 \right) &\longleftarrow (x, y).
\end{aligned}$$

Having done it, by the substitution

$$(x, y) \xrightarrow{l} (l_x, l_y) := \left(u_0 u_1^2 \left(x + \frac{3A^2 \delta(\mathfrak{g}) + c_7}{c_1} \right), u_0 u_1^3 y - \frac{a \delta(\mathfrak{g}) l_x - N_{K/F}(\gamma(\mathcal{X}_H^0))}{2} \right),$$

we achieve the Weierstrass form defining $\mathcal{W}(\mathcal{X}_H^0)$. Thus the composed map $\theta := l \circ \Theta \circ i; \mathcal{X}_H^0 \xrightarrow{\sim} \mathcal{W}(\mathcal{X}_H^0)$ is the desired one. Since the all is standard manner, the precise proof is omitted. \square

Lemma 3.7. *Let $H : a(x - w) + by + cz = 0$ be a hyperplane in \mathbb{P}^3 defined over F . Assume $at + 3c = 0$ and $at + 3b \neq 0$. Then there is a birational map given by*

$$\begin{aligned} \theta : \mathcal{X}_H^0 &\xrightarrow{\sim} \mathcal{W}(\mathcal{X}_H^0); \\ [x, y, z, w] &\longmapsto [\theta_X, \theta_Y, \theta_Z], \\ [\theta_X^{(-1)}, \theta_Y^{(-1)}, \theta_Z^{(-1)}, \theta_W^{(-1)}] &\longleftarrow [x, y, z], \\ \begin{cases} \theta_X = u_0 u_1^2 \left(\frac{z - 3c_0 w}{h_0(x, y, z, w)} + \frac{3A^2 \delta(\mathfrak{g}) + c_7}{c_1} \right) w, \\ \theta_Y = u_0 u_1^3 \left(\frac{2}{3} g_3 \left[\frac{z - 3c_0 w}{h_0(x, y, z, w)} \right] h_0(x, y, z, w) + g_2 \left[\frac{z - 3c_0 w}{h_0(x, y, z, w)} \right] \right) w - \frac{a \delta(\mathfrak{g}) \theta_X - N_{K/F}(\gamma(\mathcal{X}_H^0)) w}{2}, \\ \theta_Z = w, \end{cases} \\ \begin{cases} \theta_X^{(-1)} = (1 + t(-A + h_1(x, z))) h_2(x, y, z) z + (1 + t c_0) z, \\ \theta_Y^{(-1)} = -3A h_2(x, y, z) z, \\ \theta_Z^{(-1)} = 3(h_1(x, z) h_2(x, y, z) + c_0) z, \\ \theta_W^{(-1)} = z. \end{cases} \end{aligned}$$

Here the functions $h_0(x, y, z, w)$, $h_1(x, z)$, $h_2(x, y, z) \in F(x, y, z, w)$ and $g_3[X] \in F[X]$ have the same notation as in Lemma 3.6, but $g_2[X] = 6\delta(\mathfrak{g})X^2 + 3\frac{c_5}{c_1}\delta(\mathfrak{g})X + 3A\frac{c_6}{c_1}\delta(\mathfrak{g}) + 3$ and the constants are redefined as follows.

$$\begin{aligned} A &= \frac{a}{at + 3b}, \quad c_0 = \frac{3}{c_1}, \quad u_0 = -12\delta(\mathfrak{g})c_1, \quad u_1 = \frac{at + 3b}{18}, \\ c_1 &= -2t - 3, \quad c_2 = -A(t + 6) - 1, \quad c_3 = A(t - 3) - 1, \quad c_4 = (3A)^3 \mathfrak{g} \left(\frac{1 - At}{3A} \right), \\ c_5 &= -A(4t + 33) - 6, \quad c_6 = A(5t - 6) - 3, \quad c_7 = -A(t + 6) - 2. \end{aligned}$$

Proof. This is almost similar to the previous lemma. The substitution i defined in the previous lemma maps the hyperplane $H : a(x - w) + by + cz = 0$ to the hyperplane $i(H) : a(x - w) + (at + 3b)y + (at + 3c)z = 0$. From the assumption $at + 3c = 0$, $at + 3b \neq 0$, we have the cubic form ${}^i f_H(x, z, w) := {}^i f(x, -A(x - w), z, w)$ defining $i(\mathcal{X}_H^0) \hookrightarrow \mathbb{P}^2$. Applying the same method yields the birational map

$$\begin{aligned} \Theta : i(\mathcal{X}_H^0) &\xrightarrow{\sim} \mathcal{C} \\ (x, z) &\longmapsto \left(\frac{z - c_0}{x - 1}, 2g_3 \left[\frac{z - c_0}{x - 1} \right] (x - 1) + g_2 \left[\frac{z - c_0}{x - 1} \right] \right), \\ \left(\frac{y - g_2[x]}{2g_3[x]} + 1, \frac{y - g_2[x]}{2g_3[x]} x + c_0 \right) &\longleftarrow (x, y). \end{aligned}$$

where the curve \mathcal{C} is defined by the equation

$$y^2 = g_2[x]^2 - 4g_1[x]g_3[x].$$

Here $g_d[x]$ denotes the homogeneous part of degree d of the polynomial $g_H(1, x)$ where $g_H(x, z) := {}^i f_H(x + 1, z + c_0, 1)$. In order to obtain the required Weierstrass form, we make the substitution

$$(x, y) \xrightarrow{l} (l_x, l_y) := \left(u_0 u_1^2 \left(x + \frac{3A^2 \delta(\mathfrak{g}) + c_7}{c_1} \right), u_0 u_1^3 y - \frac{a \delta(\mathfrak{g}) l_x - N_{K/F}(\gamma(\mathcal{X}_H^0))}{2} \right).$$

This yields the desired birational map $\theta := l \circ \Theta \circ i; \mathcal{X}_H^0 \xrightarrow{\sim} \mathcal{W}(\mathcal{X}_H^0)$. \square

Remark 3.8. As for the precise proof of the above lemmas, it might be required to use the explicit calculation

$$\begin{aligned} & N_{K/F}(\gamma(\mathcal{X}_H^0)) \\ &= \frac{\delta(\mathfrak{g})}{3^3} \left(-(at+3c)^3 \mathfrak{g}(-B) - a^3 \delta(\mathfrak{g})^2 + a((at+3c)^2 + (at+3c)(at+3b) + (at+3b)^2) \delta(\mathfrak{g}) \right) \\ &= \delta(\mathfrak{g}) \left(-c^3 \mathfrak{g}\left(\frac{-b}{c}\right) - a^3(2t+3) + a^2 t(bt+3b+3c) + a(b^2(2t+3) - bc(t^2+t-3) - c^2(t-3)) \right). \end{aligned}$$

Lemma 3.9. Let $H : a(x-w) + by + cz = 0$ be a hyperplane in \mathbb{P}^3 defined over F . Assume $at+3c = at+3b = 0$. Then the hyperplane H is tangent to \mathcal{X}^0 at \mathcal{O} (i.e. \mathcal{X}_H^0 is singular from Lemma 2.3), and there is a birational map given by

$$\begin{aligned} \theta : \mathcal{X}_H^0 &\xrightarrow{\sim} \mathbb{P}^1; \\ [x, y, z, w] &\longmapsto [y, z], \\ \left[-\frac{3t(x^3+y^3)}{(x+y)^3 \mathfrak{g}\left(\frac{2y-x}{x+y}\right)} + 1, -\frac{9x(x^2-xy+y^2)}{(x+y)^3 \mathfrak{g}\left(\frac{2y-x}{x+y}\right)}, -\frac{9y(x^2-xy+y^2)}{(x+y)^3 \mathfrak{g}\left(\frac{2y-x}{x+y}\right)}, 1 \right] &\longleftarrow [x, y]. \end{aligned}$$

Proof. Since $a \neq 0$ by assumption, the defining equation of H is also written as $3(x-w) - ty - tz = 0$. But we have $\left[\frac{\partial f}{\partial x}(\mathcal{O}), \frac{\partial f}{\partial y}(\mathcal{O}), \frac{\partial f}{\partial z}(\mathcal{O}), \frac{\partial f}{\partial w}(\mathcal{O})\right] = [3, -t, -t, -3]$, which implies that H is tangent to \mathcal{X}^0 at \mathcal{O} . It is directly verified the birationality of the map. Note that the equality $(y+z)^3 \mathfrak{g}\left(\frac{2z-y}{y+z}\right) = -9(y^2 - yz + z^2)$ holds for any $[x, y, z, w] \in \mathcal{X}_H^0$. \square

Remark 3.10. As for the above, the unique singular point on the cubic curve \mathcal{X}_H^0 is \mathcal{O} .

Remark 3.11. From Corollary 3.1, the cubic curve $\mathcal{W}(\mathcal{X}_H^0)/F$ is singular if and only if $\Delta(\mathcal{X}_H^0) = 0$ which is equivalent to $A = \frac{\mathfrak{g}(-B)}{(B^2+B+1)\delta(\mathfrak{g})}$ in the case $at+3c \neq 0$. Thus the equation defining H is described as

$$\frac{\mathfrak{g}(-B)}{(B^2+B+1)\delta(\mathfrak{g})} (3(x-w) - ty - tz) + By + z = 0.$$

By direct calculation, one can find that the hyperplane H coincides with the tangent plane to \mathcal{X}^0 at the point

$$t \begin{pmatrix} (-B^6(t+2) - 3B^5(t+3) - 6B^4(t+4) + B^3(t^2+t-23) + 3B^2(t-3) - 3B-2) \mathfrak{g}(-B)^{-2} \\ (B^2+B+1)(-B^4-2B^3-6B^2+2B(t-1)+t+2) \mathfrak{g}(-B)^{-2} \\ (B^2+B+1)(B^4(t+1)+2B^3(t+4)+6B^2+2B+1) \mathfrak{g}(-B)^{-2} \end{pmatrix}.$$

Therefore this is the only singular point on \mathcal{X}_H^0 . In the case $at+3c = 0$, $at+3b \neq 0$, since $\Delta(\mathcal{X}_H^0) = 0$ is equivalent to $A = -\frac{1}{\delta(\mathfrak{g})}$, the hyperplane is

$$-\frac{1}{\delta(\mathfrak{g})}(x-w) + y = 0.$$

This is the tangent plane to \mathcal{X}^0 at the point $(-t-2, -1, t+1)$, which is singular on \mathcal{X}_H^0 . These also assure Lemma 2.3 once again.

Lemma 3.12. Assume $H \in \mathcal{L}(\mathcal{O})$ is not tangent to \mathcal{X}^0 . Then $\theta(\mathcal{O}) = [0, 1, 0]$ where $\theta : \mathcal{X}_H^0 \rightarrow \mathcal{W}(\mathcal{X}_H^0)$ is the map in Lemma 3.6 or 3.7. Especially θ is a group isomorphism.

Proof. It suffices to prove the lemma for the map Θ defined in the proof of Lemma 3.6 or 3.7 since $\theta = l \circ \Theta \circ i$ and $i(\mathcal{O}) = \mathcal{O}$, $l([0, 1, 0]) = [0, 1, 0]$. First assume $at + 3c \neq 0$. Under the assumption, the ring $F[i(\mathcal{X}_H^0)]_{\mathcal{O}}$ of regular functions on $i(\mathcal{X}_H^0)$ at \mathcal{O} is a discrete valuation ring. Since the x -coordinate of the map Θ is the function $\frac{y-c_0}{x-1}$ which has a pole at \mathcal{O} , multiplying an appropriate power of a uniformizer for $F[i(\mathcal{X}_H^0)]_{\mathcal{O}}$ to the projective coordinate of Θ yields $\Theta(\mathcal{O}) = [0, 1, 0]$. In the case $at + 3c = 0$ and $at + 3b \neq 0$, the x -coordinate of the map Θ is the function $\frac{z-c_0}{x-1}$. We also have $\Theta(\mathcal{O}) = [0, 1, 0]$ similarly. The statement is now proven. \square

Proof of Theorem 1.1. Fix arbitrary cyclic cubic extension K/F . Let \mathcal{X} be a cubic hypersurface associated to K/F with a F -basis $\{1, \alpha_1, \alpha_2\}$ of K defined by the polynomial (1.1) and \mathcal{X}^0 as above. Then the transformation matrix $M \in \mathrm{GL}_3(F)$ with $(1, \alpha, \alpha^\sigma)M = (1, \alpha_1, \alpha_2)$ defines a regular transformation \widetilde{M} on \mathbb{P}^3 given by $[x, y, z, w] \mapsto [x, y, z, w] \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$, whose restriction induces an isomorphism $\mathcal{X}_H \xrightarrow{\sim} \mathcal{X}_{H'}^0$ where $H' = \widetilde{M}(H)$ has the form $a'(x-w) + b'y + c'z = 0$ with $(a', b', c')M = (a, b, c)$. We thus obtain $\delta(\mathcal{X}^0)|M| = \delta(\mathcal{X})$, $\gamma(\mathcal{X}_{H'}^0)|M| = \gamma(\mathcal{X}_H)$ and $a' = a$. From this and Lemma 3.6, 3.7, the composed map

$$(3.1) \quad \vartheta : \mathcal{X}_H \xrightarrow{\widetilde{M}} \mathcal{X}_{H'}^0 \xrightarrow{\theta} \mathcal{W}(\mathcal{X}_{H'}^0) \xrightarrow{m} \mathcal{W}(\mathcal{X}_H)$$

is the required one. Here m denotes the map $(x, y) \mapsto (|M|^2x, |M|^3y)$. It follows from Lemma 3.12 that $\vartheta(\mathcal{O}) = [0, 1, 0]$. \square

Proposition 3.13. $\vartheta(\mathcal{O}'^\sigma - \mathcal{O}') = \pm(0, 0)$.

Proof. From (3.1), it suffices to prove the statement for the map $\theta : \mathcal{X}_H^0 \rightarrow \mathcal{W}(\mathcal{X}_H^0)$ since $\widetilde{M}(c\alpha_1 - b\alpha_2, a\alpha_2 - c, -a\alpha_1 + b, 0) = [c'\alpha - b'\frac{1}{1-\alpha}, a'\frac{1}{1-\alpha} - c', -a'\alpha + b', 0]$. Let $V_F := \{\alpha \in \overline{F} \setminus F \mid \mathfrak{g}(\alpha; t) = 0 \text{ for some } t \in F\}$, and for any $\alpha \in V_F$ let $S_\alpha \subset \mathbb{A}^3$ be a hypersurface in variables a, b, c defined by the equation (cf. Remark 3.11)

$$\left(-N_{K/F}(\gamma(\mathcal{X}_H^0))^{-3} \Delta(\mathcal{X}_H^0)\right) a^3 \delta(\mathcal{X}^0)^3 + 3^3 N_{K/F}(\gamma(\mathcal{X}_H^0)) = 0$$

where \mathcal{X}^0 is associated to $F(\alpha)/F$ with the F -basis $\{1, \alpha, \frac{1}{1-\alpha}\}$ of $F(\alpha)$ and H is a hyperplane $a(x-w) + by + cz = 0$. Let $\mathcal{O}'' := [c\frac{1}{1-\alpha} - b(1-\frac{1}{\alpha}), a(1-\frac{1}{\alpha}) - c, -a\frac{1}{1-\alpha} + b, 0]$ on \mathcal{X}_H^0 and $P := \mathcal{O}'' - \mathcal{O}'$. Note that $\mathcal{O}'' = \mathcal{O}'^\sigma$ or \mathcal{O}'^{σ^2} since $\alpha^\sigma = \frac{1}{1-\alpha}$ or $1 - \frac{1}{\alpha}$ from §8. Thus $P \in \mathcal{X}_H^0(F) \setminus \{\mathcal{O}\}$ by Lemma 2.4. For the map $\theta = [\theta_X, \theta_Y, \theta_Z]$ as in Lemma 3.6 or 3.7, we can regard $(\theta_x, \theta_y) := (\frac{\theta_X}{\theta_Z}(P), \frac{\theta_Y}{\theta_Z}(P))$ as functions in variables a, b, c, α , namely $\theta_x, \theta_y \in \mathbb{Q}(x_1, x_2, x_3, x_4)$. This makes the rational map

$$\begin{aligned} \varphi : \mathbb{A}^4 &\longrightarrow \mathbb{A}^2 \\ (a, b, c, \alpha) &\longmapsto (\theta_x(a, b, c, \alpha), \theta_y(a, b, c, \alpha)). \end{aligned}$$

For any $\alpha_0 \in V_{\mathbb{Q}}$, let $\varphi|_{\alpha_0} : \mathbb{A}^3 \rightarrow \mathbb{A}^2$ be the restriction map to $\alpha = \alpha_0$. Then the Weil pairing tells us $\varphi|_{\alpha_0}(a, b, c) = \pm(0, 0)$ on $\mathbb{A}^3(\mathbb{Q}) \setminus S_{\alpha_0}(\mathbb{Q})$ by using Lemma 2.4, Corollary 3.2 and $\zeta_3 \notin \mathbb{Q}$. Thus the rational functions $\theta_x|_{\alpha_0}, \theta_y|_{\alpha_0}$ are constant for infinitely many values a, b, c respectively, and hence $\theta_x|_{\alpha_0}, \theta_y|_{\alpha_0}$ must be constants in $\overline{\mathbb{Q}}(x_1, x_2, x_3)$. It turns out that the map φ depends only on the variable x_4 . However φ also takes $\pm(0, 0)$ for infinitely many $\alpha \in V_{\mathbb{Q}}$, which implies that φ is a constant map taking the image either $(0, 0)$ or $-(0, 0)$. Especially, for any number field F , the evaluation of φ for $\alpha \in V_F$ and $(a, b, c) \in \mathbb{A}^3(F) \setminus S_\alpha(F)$ yields the required result. \square

4. Descent theory for \mathcal{X}_H via 3-isogeny

We shall now discuss descent theory for the elliptic curve \mathcal{X}_H over F . Fix \mathcal{O} as a base point of \mathcal{X}_H . Then the set of F -rational points $\mathcal{X}_H(F)$, often called Mordell-Weil group, is a finitely generated abelian group with group unit \mathcal{O} , whose structure does not depend on the choice of a base point. It is one of the main interest to know the rank of $\mathcal{X}_H(F)$. If one could calculate the quotient group $\mathcal{X}_H(F)/m\mathcal{X}_H(F)$ for some integer $m > 1$, one could find the rank of $\mathcal{X}_H(F)$. Descent theory gives an upper bound for the size of the quotient group $\mathcal{X}_H(F)/m\mathcal{X}_H(F)$, which often gives the exact size. At the beginning, we make notation used in the present paper and recall some basic objects on descent theory in the case $m = 3$, which we call 3-descent.

From Proposition 3.13, we may assume $\vartheta(\mathcal{O}'^\sigma - \mathcal{O}') = (0, 0)$ without loss of generality by the proper substitution either $\vartheta \leftrightarrow [-1] \circ \vartheta$ or $\sigma \leftrightarrow \sigma^2$.

Let $\phi : \mathcal{X}_H \rightarrow \widehat{\mathcal{X}_H}$ be a 3-isogeny defined over F with the dual elliptic curve $\widehat{\mathcal{X}_H} := \mathcal{X}_H/\langle T \rangle$ where $T := \mathcal{O}'^\sigma - \mathcal{O}'$, and let $\widehat{\phi} : \widehat{\mathcal{X}_H} \rightarrow \mathcal{X}_H$ be its dual isogeny which is also defined over F . For the short exact sequence $0 \rightarrow \mathcal{X}_H[\phi] \rightarrow \mathcal{X}_H(\overline{F}) \xrightarrow{\phi} \widehat{\mathcal{X}_H}(\overline{F}) \rightarrow 0$ as G_F -modules where G_F denotes an absolute Galois group of F , taking Galois cohomology yields the exact sequence

$$0 \longrightarrow \widehat{\mathcal{X}_H}(F)/\phi(\mathcal{X}_H(F)) \longrightarrow H^1(F, \mathcal{X}_H[\phi]) \longrightarrow H^1(F, \mathcal{X}_H)[\phi] \longrightarrow 0.$$

Considering the above locally again, we also have a similar localized exact sequence. For the completion $F_{\mathfrak{p}}$ at each prime \mathfrak{p} of F , since an embedding $\overline{F} \hookrightarrow \overline{F}_{\mathfrak{p}}$, which may be fixed once and for all, induces restriction maps of Galois cohomology, we obtain the following commutative diagram.

$$\begin{array}{ccccccc} 0 & \longrightarrow & \widehat{\mathcal{X}_H}(F)/\phi(\mathcal{X}_H(F)) & \xrightarrow{\delta} & H^1(F, \mathcal{X}_H[\phi]) & \longrightarrow & H^1(F, \mathcal{X}_H)[\phi] \longrightarrow 0 \\ & & \downarrow \text{res}_{\mathfrak{p}} & & \downarrow \text{res}_{\mathfrak{p}} & & \downarrow \text{res}_{\mathfrak{p}} \\ 0 & \longrightarrow & \widehat{\mathcal{X}_H}(F_{\mathfrak{p}})/\phi(\mathcal{X}_H(F_{\mathfrak{p}})) & \xrightarrow{\delta_{\mathfrak{p}}} & H^1(F_{\mathfrak{p}}, \mathcal{X}_H[\phi]) & \longrightarrow & H^1(F_{\mathfrak{p}}, \mathcal{X}_H)[\phi] \longrightarrow 0 \end{array}$$

where $\delta, \delta_{\mathfrak{p}}$ stand for connecting homomorphisms of Galois cohomology. The ϕ -Selmer group of the elliptic curve \mathcal{X}_H is a finite subgroup of $H^1(F, \mathcal{X}_H[\phi])$ defined by

$$S^{(\phi)}(\mathcal{X}_H/F) = \left\{ \bar{\xi} \in H^1(F, \mathcal{X}_H[\phi]) \mid \text{res}_{\mathfrak{p}}(\bar{\xi}) \in \text{Im } \delta_{\mathfrak{p}} \text{ for any finite/infinite prime } \mathfrak{p} \text{ of } F \right\}.$$

It is clear by the above diagram that the group $S^{(\phi)}(\mathcal{X}_H/F)$ contains $\widehat{\mathcal{X}_H}(F)/\phi(\mathcal{X}_H(F))$ as subgroup. The gap between these groups is represented by the ϕ -kernel of the Shafarevich-Tate group, which sits in the exact sequence

$$0 \longrightarrow \widehat{\mathcal{X}_H}(F)/\phi(\mathcal{X}_H(F)) \longrightarrow S^{(\phi)}(\mathcal{X}_H/F) \longrightarrow \text{III}(\mathcal{X}_H/F)[\phi] \longrightarrow 0.$$

Oppositely, one can define the $\widehat{\phi}$ -Selmer group $S^{(\widehat{\phi})}(\widehat{\mathcal{X}_H}/F)$ and the $\widehat{\phi}$ -kernel of the Shafarevich-Tate group $\text{III}(\widehat{\mathcal{X}_H}/F)[\widehat{\phi}]$ on interchanging the role of the isogenies $\phi, \widehat{\phi}$.

A relation between the finite groups $\widehat{\mathcal{X}}_H(F)/\phi(\mathcal{X}_H(F))$ and $\mathcal{X}_H(F)/\widehat{\phi}(\widehat{\mathcal{X}}_H(F))$ is described by the exact sequence

$$0 \longrightarrow \frac{\widehat{\mathcal{X}}_H(F)[\widehat{\phi}]}{\phi(\mathcal{X}_H(F)[3])} \longrightarrow \frac{\widehat{\mathcal{X}}_H(F)}{\phi(\mathcal{X}_H(F))} \xrightarrow{\widehat{\phi}} \frac{\mathcal{X}_H(F)}{3\mathcal{X}_H(F)} \longrightarrow \frac{\mathcal{X}_H(F)}{\widehat{\phi}(\widehat{\mathcal{X}}_H(F))} \longrightarrow 0.$$

It is easily seen that $\frac{\widehat{\mathcal{X}}_H(F)[\widehat{\phi}]}{\phi(\mathcal{X}_H(F)[3])} \simeq \mathbb{Z}/3\mathbb{Z}$ if and only if $\zeta_3 \in F$ and $\mathcal{X}_H(F)[3] = \mathcal{X}_H(F)[\phi] \simeq \mathbb{Z}/3\mathbb{Z}$. From this we have the formula

$$(4.1) \quad \text{rank}_{\mathbb{Z}} \mathcal{X}_H(F) = \dim_{\mathbb{F}_3} \frac{\mathcal{X}_H(F)}{\widehat{\phi}(\widehat{\mathcal{X}}_H(F))} + \dim_{\mathbb{F}_3} \frac{\widehat{\mathcal{X}}_H(F)}{\phi(\mathcal{X}_H(F))} - \dim_{\mathbb{F}_3} \mu_3(F) - 1.$$

Thus the Selmer groups give an upper bound for the rank of the Mordell-Weil group. From now on, to estimate the size of the rank, we consider the Selmer groups.

4.1. On the Selmer group $S^{(\phi)}(\mathcal{X}_H/F)$ Since $\mathcal{X}_H[\phi] \subset \mathcal{X}_H(F)$, one sees that

$$H^1(F, \mathcal{X}_H[\phi]) \simeq H^1(F, C_3) = \text{Hom}(G_F, C_3).$$

Here the Galois action on the cyclic group $C_3 \simeq \mathbb{Z}/3\mathbb{Z}$ is regarded as trivial one. Define the set of all cyclic cubic extensions over F together with F by

$$\mathfrak{Gal}(C_3/F) := \left\{ L/F : \text{Galois extension} \mid \text{Gal}(L/F) \hookrightarrow C_3 \right\} / \{\text{isomorphisms}\}.$$

Then there is the surjection $\text{Hom}(G_F, C_3) \rightarrow \mathfrak{Gal}(C_3/F); \xi \mapsto \overline{F}^{\text{Ker } \xi}$. We thus obtain the composed map

$$\delta_F : \widehat{\mathcal{X}}_H(F)/\phi(\mathcal{X}_H(F)) \xrightarrow{\delta} H^1(F, \mathcal{X}_H[\phi]) \simeq \text{Hom}(G_F, C_3) \longrightarrow \mathfrak{Gal}(C_3/F).$$

Considering locally again, we have the commutative diagram

$$\begin{array}{ccc} \widehat{\mathcal{X}}_H(F)/\phi(\mathcal{X}_H(F)) & \xrightarrow{\delta_F} & \mathfrak{Gal}(C_3/F) \\ \downarrow \text{resp} & & \downarrow \text{resp} \\ \widehat{\mathcal{X}}_H(F_{\mathfrak{p}})/\phi(\mathcal{X}_H(F_{\mathfrak{p}})) & \xrightarrow{\delta_{F_{\mathfrak{p}}}} & \mathfrak{Gal}(C_3/F_{\mathfrak{p}}). \end{array}$$

The following gives a slightly different description for the ϕ -Selmer group.

Proposition 4.1. *The map $\delta_{F_{\bullet}}$ is explicitly written as*

$$\begin{aligned} \delta_{F_{\bullet}} : \widehat{\mathcal{X}}_H(F_{\bullet})/\phi(\mathcal{X}_H(F_{\bullet})) &\longrightarrow \mathfrak{Gal}(C_3/F_{\bullet}) \\ P &\longmapsto F_{\bullet}(\phi^{-1}(P)). \end{aligned}$$

Here \bullet stands for \mathfrak{p} or null space. Moreover it holds that

$$\sharp S^{(\phi)}(\mathcal{X}_H/F) = 2 \cdot \sharp \left\{ L \in \mathfrak{Gal}(C_3/F) \mid \begin{array}{l} L/F \text{ is unramified outside } S_0 \\ L \cdot F_{\mathfrak{p}} \in \text{Im } \delta_{F_{\mathfrak{p}}} \text{ for any } \mathfrak{p} \in S_0 \end{array} \right\} - 1$$

where S_0 denotes the set of finite primes of F at which \mathcal{X}_H has bad reduction or dividing 3.

Proof. By tracing the definitions and consequences of descent theory. For details, see [9], §2. \square

Remark 4.2. Since $\mathcal{X}_H(F)[\phi] = \langle \mathcal{O}'^\sigma - \mathcal{O}' \rangle$ by the definition, the point $P = \phi(\mathcal{O}') \in \widehat{\mathcal{X}_H}$ is F -rational. For any cyclic cubic extension K/F and any hyperplane $H \in \mathcal{L}(\mathcal{O})$ not tangent to \mathcal{X} , taking such $P \in \widehat{\mathcal{X}_H}(F)$ yields $\delta_F(P) = F(\mathcal{O}') = K$. Thus all cyclic cubic extensions over F are subject to F -rational points on the elliptic curves $\{\widehat{\mathcal{X}_H}/F\}$. Furthermore it is also observed that the elliptic curve \mathcal{X}_H/F has bad reduction at each prime $\mathfrak{p} \nmid 3$ which ramifies in K .

4.2. On the Selmer group $S^{(\widehat{\phi})}(\widehat{\mathcal{X}_H}/F)$ As for the dual side, the Weil pairing $e_{\widehat{\phi}}$ for the isogeny $\widehat{\phi}$ constructs the commutative diagram

$$\begin{array}{ccccc} \mathcal{X}_H(F)/\widehat{\phi}(\widehat{\mathcal{X}_H}(F)) & \xrightarrow{\widehat{\delta}} & H^1(F, \widehat{\mathcal{X}_H}[\widehat{\phi}]) & \xrightarrow{e_{\widehat{\phi}}(\cdot, T)} & H^1(F, \mu_3) \simeq F^*/F^{*3} \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{X}_H(K)/\widehat{\phi}(\widehat{\mathcal{X}_H}(K)) & \xrightarrow{\widehat{\delta}} & H^1(K, \widehat{\mathcal{X}_H}[\widehat{\phi}]) & \xrightarrow{e_{\widehat{\phi}}(\cdot, T)} & H^1(K, \mu_3) \simeq K^*/K^{*3}. \end{array}$$

We denote by $\widehat{\delta}_F, \widehat{\delta}_F^K$ the homomorphisms from the group $\mathcal{X}_H(F)/\widehat{\phi}(\widehat{\mathcal{X}_H}(F))$ to $F^*/F^{*3}, K^*/K^{*3}$ respectively. For each finite prime \mathfrak{p} of F , it may be defined similarly the maps $\widehat{\delta}_{F_{\mathfrak{p}}} : \mathcal{X}_H(F_{\mathfrak{p}})/\widehat{\phi}(\widehat{\mathcal{X}_H}(F_{\mathfrak{p}})) \rightarrow F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*3}$ and $\widehat{\delta}_{F_{\mathfrak{p}}}^{K_{\mathfrak{p}}} : \mathcal{X}_H(F_{\mathfrak{p}})/\widehat{\phi}(\widehat{\mathcal{X}_H}(F_{\mathfrak{p}})) \rightarrow K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*3}$ where \mathfrak{P} is a prime of K above \mathfrak{p} . There is no need to consider infinite primes since $H^1(F_{\infty}, \widehat{\mathcal{X}_H}[\widehat{\phi}])$ vanishes. Thus the $\widehat{\phi}$ -Selmer group can be rewritten as

$$S^{(\widehat{\phi})}(\widehat{\mathcal{X}_H}/F) = \left\{ \overline{d} \in F^*/F^{*3} \mid \overline{d} \in \text{Im } \widehat{\delta}_{F_{\mathfrak{p}}} \text{ for any finite prime } \mathfrak{p} \text{ of } F \right\}.$$

Let $\mathcal{K}_{\mathfrak{p}}$ denote the étale algebra $F_{\mathfrak{p}}[x]/(\mathfrak{g}(x; t))$, where \mathfrak{g} is the generic polynomial in §8, which is isomorphic to the direct sum of the completions $K_{\mathfrak{P}}$ of K at the primes \mathfrak{P} lying above \mathfrak{p} , namely $\mathcal{K}_{\mathfrak{p}} \simeq \prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}} \simeq K \otimes_F F_{\mathfrak{p}}$, and let $\mathcal{K}_{\mathfrak{p}}^*$ denote the multiplicative group $\prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^*$. We frequently use the identification $\mathcal{K}_{\mathfrak{p}}^*/\mathcal{K}_{\mathfrak{p}}^{*3} \simeq \prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^*/K_{\mathfrak{P}}^{*3}$. The natural inclusion $F \subset F_{\mathfrak{p}}$ induces an embedding $K \hookrightarrow \mathcal{K}_{\mathfrak{p}}$ by the identification $K = F[x]/(\mathfrak{g}(x; t))$. We define a map $\widehat{\delta}_{F_{\mathfrak{p}}}^{\mathcal{K}_{\mathfrak{p}}} : \mathcal{X}_H(F_{\mathfrak{p}})/\widehat{\phi}(\widehat{\mathcal{X}_H}(F_{\mathfrak{p}})) \rightarrow \mathcal{K}_{\mathfrak{p}}^*/\mathcal{K}_{\mathfrak{p}}^{*3}$ by $P \mapsto \prod_{\mathfrak{P}|\mathfrak{p}} \widehat{\delta}_{F_{\mathfrak{p}}}^{K_{\mathfrak{P}}}(P)$ which commutes the diagram

$$\begin{array}{ccccc} \widehat{\delta}_F^K : \mathcal{X}_H(F)/\widehat{\phi}(\widehat{\mathcal{X}_H}(F)) & \xrightarrow{\widehat{\delta}_F} & F^*/F^{*3} & \longrightarrow & K^*/K^{*3} \\ \downarrow & & \downarrow & & \downarrow \\ \widehat{\delta}_{F_{\mathfrak{p}}}^{\mathcal{K}_{\mathfrak{p}}} : \mathcal{X}_H(F_{\mathfrak{p}})/\widehat{\phi}(\widehat{\mathcal{X}_H}(F_{\mathfrak{p}})) & \xrightarrow{\widehat{\delta}_{F_{\mathfrak{p}}}} & F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*3} & \longrightarrow & \mathcal{K}_{\mathfrak{p}}^*/\mathcal{K}_{\mathfrak{p}}^{*3}. \end{array}$$

As for the maps $\widehat{\delta}_F^K, \widehat{\delta}_{F_{\mathfrak{p}}}^{\mathcal{K}_{\mathfrak{p}}}$, we will give a certain description in Proposition 6.3 which is essential in §5. Note that the homomorphisms $\widehat{\delta}_F, \widehat{\delta}_{F_{\mathfrak{p}}}$ are injective from the non-degeneracy of the Weil pairing $e_{\widehat{\phi}}$ but $\widehat{\delta}_F^K, \widehat{\delta}_{F_{\mathfrak{p}}}^{\mathcal{K}_{\mathfrak{p}}}$ are not necessarily, because the natural maps $F^*/F^{*3} \rightarrow K^*/K^{*3}$ and $F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*3} \rightarrow K_{\mathfrak{P}}^*/K_{\mathfrak{P}}^{*3}$ are not injective in general. See also Lemma 7.1.

The following lemma is proven via local consideration by applying the Hasse principle for norm varieties, which was originally proven in [7].

Lemma 4.3. $S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/F) \subset N_{K/F}(K^*)/F^{*3}.$

Proof. For arbitrary $\bar{d} \in S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/F)$, it suffices to show $d \in N_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}(K_{\mathfrak{p}}^*)$ for every prime of F by Hasse norm theorem. This is immediate for infinite primes or finite primes which split completely in K . We thus assume a finite prime \mathfrak{p} does not split completely in K . Then $\text{Gal}(K_{\mathfrak{p}}/F_{\mathfrak{p}}) \simeq \text{Gal}(K/F)$. Since d represents an element in $S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/F)$, there is a point $[x, y, z, 1] \in \mathcal{X}_H(F_{\mathfrak{p}})$ and some element $\beta \in K_{\mathfrak{p}}^*$ such that $d = \frac{x+y\alpha_1^{\sigma}+z\alpha_2^{\sigma}}{x+y\alpha_1+z\alpha_2}\beta^3$ from Proposition 6.3. Note here that $\mathcal{X}_H(F_{\mathfrak{p}}) \cap \{w=0\} = \emptyset$ if and only if $F_{\mathfrak{p}} \neq K_{\mathfrak{p}}$. From Lemma 7.2 we have $N_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}(\beta) = d$. Gathering all the pieces, we can conclude $d \in N_{K/F}(K^*)$. \square

Remark 4.4. From the above we have $\text{Im } \hat{\delta}_F \subset N_{K/F}(K^*)/F^{*3}.$

4.3. Combining the Selmer groups $S^{(\phi)}(\mathcal{X}_H/F)$ and $S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/F)$ Given an isogeny and its dual isogeny, it is known Cassels's duality formula in [3] which connects order of a Selmer group with that of its dual Selmer group. Applying the result in [9] yields the following connection formula. However, for simplicity, we consider only the case $a=0$ which we will use later, namely the hyperplane $H : by + cz = 0$ with coefficients $[b, c] \in \mathbb{P}^1(\mathfrak{O}_F)$.

Proposition 4.5. *Assume F has class number 1 in which 3 splits completely. Let $v_{\mathfrak{p}} := \nu_{\mathfrak{p}}(N_{K/F}(\gamma(\mathcal{X}_H))) \in \mathbb{Z}$ for $\mathfrak{p} \in \mathcal{P}_F$ where \mathcal{P}_F stands for the set of all finite primes of F . For a hyperplane $H : by + cz = 0$ which is not tangent to \mathcal{X} , it holds that*

$$\dim_{\mathbb{F}_3} S^{(\phi)}(\mathcal{X}_H/F) = \dim_{\mathbb{F}_3} S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/F) + d_+ - d_- + d_{\infty} - r$$

where r denotes the rank of the group \mathfrak{O}_F^* of units and

$$\begin{aligned} d_+ &:= \#\left\{\mathfrak{p} \in \mathcal{P}_F \mid \mathfrak{p} \mid 3 \text{ and } N_{K/F}(\gamma(\mathcal{X}_H)) \in F_{\mathfrak{p}}^{*3}\right\}, \\ d_- &:= \#\left\{\mathfrak{p} \in \mathcal{P}_F \mid 3 \nmid v_{\mathfrak{p}} \text{ and } \{\mathfrak{p} \mid 3 \text{ or } \zeta_3 \notin F_{\mathfrak{p}}\}\right\}, \\ d_{\infty} &:= \#\left\{\mathfrak{p} \in \mathcal{P}_F \mid v_{\mathfrak{p}} \equiv 2 \pmod{3} \text{ and } \mathfrak{p} \mid 3\right\}. \end{aligned}$$

Proof. This is a direct consequence from [9] combining with Cassels's duality formula. \square

Remark 4.6. Assume 3 is unramified in F . Let \mathfrak{p} be a prime of F above 3. Then, for an element $d \in F_{\mathfrak{p}}^*$, the condition $d \notin F_{\mathfrak{p}}^{*3}$ is equivalent to the condition either $3 \nmid \nu_{\mathfrak{p}}(d)$ or $3 \mid \nu_{\mathfrak{p}}(d)$, $u_{\pi} \not\equiv k_{\pi}^3 \pmod{\pi^2}$ for the constants $u_{\pi}, k_{\pi} \in \mathfrak{O}_{F_{\mathfrak{p}}}^*$ which are defined to be $u_{\pi} \equiv k_{\pi}^3 \pmod{\pi}$ with $u_{\pi} := \pi^{-\nu_{\mathfrak{p}}(d)}d$ where π stands for a prime element in $F_{\mathfrak{p}}$. Further we assume 3 splits completely in F . Then u_{π} is equivalent to ± 1 modulo π and hence we can choose $k_{\pi} = \pm 1$ respectively.

5. Unit groups, Class groups and Selmer groups

As for relations between class groups and Selmer groups, it has been investigated by many authors. For example, L. C. Washington [14] discussed the connection of Selmer groups to class groups of cyclic cubic fields over \mathbb{Q} , N. Aoki [1] of cubic extensions over arbitrary number field containing a primitive cube root of unity. E. F. Schaefer [10] also investigated the case when those groups coincide for the minimal field of definition of torsion points on abelian varieties. This section is intended to study the family of elliptic curves $\{\mathcal{X}_H\}_H$ in such direction. However, in addition to class groups, here we also take unit groups into account in view of the analogy between Mordell-Weil groups and unit groups.

For any set S of finite primes of F , and any finite extension L over F , define

$$\begin{aligned}\mathfrak{D}_{L,S} &:= \{\alpha \in L \mid \nu_{\mathfrak{P}}(\alpha) \geq 0 \text{ for any } \mathfrak{P} \in \mathcal{P}_{L,S}\}, \\ \mathfrak{R}_{L,S} &:= \{\bar{\alpha} \in L^*/L^{*3} \mid \nu_{\mathfrak{P}}(\alpha) \equiv 0 \pmod{3} \text{ for any } \mathfrak{P} \in \mathcal{P}_{L,S}\}, \\ \text{Cl}_{L,S} &:= \{\text{non-zero fractional ideals of } \mathfrak{D}_{L,S}\} / L^* \mathfrak{D}_{L,S}.\end{aligned}$$

Here $\mathcal{P}_{L,S}$ stands for the set of all finite primes of L outside S . When $S = \emptyset$, we omit the letter S as \mathcal{P}_L , \mathfrak{D}_L , \mathfrak{R}_L , Cl_L and so on. In this section, we show some connection between the Selmer group $S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/F)$ and unit groups $\mathfrak{D}_{L,S}^*$, class groups $\text{Cl}_{L,S}$ in the case $L = F$ or K . To begin with, we quote [9], Proposition 4.5, which implies the following.

Lemma 5.1. *The following equivalences hold.*

$$\begin{aligned}\text{Im } \widehat{\delta}_{F_{\mathfrak{p}}} &\hookrightarrow \mathfrak{D}_{F_{\mathfrak{p}}}^* / \mathfrak{D}_{F_{\mathfrak{p}}}^{*3} &\iff \mathfrak{p} \in \mathcal{P}_{F,S}, \\ \text{Im } \widehat{\delta}_{F_{\mathfrak{p}}}^{\mathcal{K}_{\mathfrak{p}}} &\hookrightarrow \mathfrak{D}_{\mathcal{K}_{\mathfrak{p}}}^* / \mathfrak{D}_{\mathcal{K}_{\mathfrak{p}}}^{*3} &\iff \mathfrak{p} \in \mathcal{P}_{F,S'},\end{aligned}$$

where $\mathfrak{D}_{\mathcal{K}_{\mathfrak{p}}}^* / \mathfrak{D}_{\mathcal{K}_{\mathfrak{p}}}^{*3} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{D}_{K_{\mathfrak{P}}}^* / \mathfrak{D}_{K_{\mathfrak{P}}}^{*3}$ and S, S' are finite sets defined by

$$\begin{aligned}S &:= \left\{ \mathfrak{p} \in \mathcal{P}_F \mid \begin{array}{l} 3\nu_{\mathfrak{p}}(a\delta(\mathcal{X})) < \nu_{\mathfrak{p}}(N_{K/F}(\gamma(\mathcal{X}_H))) \\ \text{or } \nu_{\mathfrak{p}}(N_{K/F}(\gamma(\mathcal{X}_H))) \not\equiv 0 \pmod{3} \end{array} \right\}, \\ S' &:= \left\{ \mathfrak{p} \in S \mid \mathfrak{p} \text{ splits completely in } K \right\}.\end{aligned}$$

Proof. The first equivalence follows directly from [9], Proposition 4.5. As for the second, for any $\mathfrak{p} \in \mathcal{P}_{F,S'}$ if \mathfrak{p} is inert or ramifies in K then $\text{Im } \widehat{\delta}_{F_{\mathfrak{p}}}^{\mathcal{K}_{\mathfrak{p}}} \hookrightarrow \mathfrak{D}_{\mathcal{K}_{\mathfrak{p}}}^* / \mathfrak{D}_{\mathcal{K}_{\mathfrak{p}}}^{*3}$ by using Proposition 6.3. If \mathfrak{p} splits completely in K then $\mathfrak{p} \in \mathcal{P}_{F,S}$, and hence the statement follows from the first equivalence since $F_{\mathfrak{p}} = K_{\mathfrak{P}}$ as valuation fields for each $\mathfrak{P} \mid \mathfrak{p}$. Conversely, for any $\mathfrak{p} \in S'$ the first equivalence implies $\text{Im } \widehat{\delta}_{F_{\mathfrak{p}}}^{\mathcal{K}_{\mathfrak{p}}} \not\hookrightarrow \mathfrak{D}_{\mathcal{K}_{\mathfrak{p}}}^* / \mathfrak{D}_{\mathcal{K}_{\mathfrak{p}}}^{*3}$. \square

By the above lemma, it turns out that each element in $S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/F)$ is of \mathfrak{P} -adic valuation divided by 3 outside S' , namely $S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/F)$ relates to the 3-torsion subgroup of the S' -ideal class group $\text{Cl}_{K,S'}$. We will also consider the relation to that of the S -ideal class group $\text{Cl}_{F,S}$.

We make notation as

$$\begin{aligned} {}_N\Phi_{F,S} &:= \frac{N_{K/F}(K^*) \cap \mathfrak{D}_{F,S}^*}{\mathfrak{D}_{F,S}^{*3}} \left(\subset \mathfrak{D}_{F,S}^* / \mathfrak{D}_{F,S}^{*3} \right), \\ {}_N\text{Cl}_{F,S}[3] &:= \left\{ \bar{\alpha} \in \text{Cl}_{F,S}[3] \mid \alpha^3 = d\mathfrak{D}_{F,S}, d \in N_{K/F}(K^*) \right\} \left(\subset \text{Cl}_{F,S}[3] \right), \\ {}_N\mathfrak{U}_{K,S'} &:= \left\{ \overline{\alpha^{\sigma-1}} \in \mathfrak{D}_{K,S'}^* K^{*3} / K^{*3} \mid \alpha \in K^*, N_{K/F}(\alpha) = 1 \right\} \left(\subset \mathfrak{D}_{K,S'}^* / \mathfrak{D}_{K,S'}^{*3} \right), \\ {}_N\text{Cl}_{K,S'}[3] &:= \left\{ \bar{\mathfrak{A}} \in \text{Cl}_{K,S'}[3] \mid \mathfrak{A}^3 = \alpha \mathfrak{D}_{K,S'}, N_{K/F}(\alpha) = 1 \right\} \left(\subset \text{Cl}_{K,S'}[3] \right). \end{aligned}$$

As is indicated, these groups are finite and subject to certain norm condition. Note that the Galois group $G = \text{Gal}(K/F)$ acts canonically on the quotient K^*/K^{*3} and the S' -ideal class group $\text{Cl}_{K,S'}$ by $\sigma(\bar{\alpha}) = \overline{\alpha^\sigma}$, $\sigma(\bar{\mathfrak{A}}) = \overline{\mathfrak{A}^\sigma}$ respectively. The purpose of this section is to prove the following results.

Theorem 5.2. *For any hyperplane $H/F \in \mathcal{L}(\mathcal{O})$ which is not tangent to \mathcal{X} , let S, S' be the finite sets in Lemma 5.1. Then there is a finite bound*

$$\begin{aligned} \dim_{\mathbb{F}_3} S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/F) &\leq \dim_{\mathbb{F}_3} {}_N\Phi_{F,S} + \dim_{\mathbb{F}_3} {}_N\text{Cl}_{F,S}[3] \\ &\leq \dim_{\mathbb{F}_3} {}_N\mathfrak{U}_{K,S'} \oplus \mu_3(F) + \dim_{\mathbb{F}_3} {}_N\text{Cl}_{K,S'}^G[3] - \dim_{\mathbb{F}_3} \frac{N_{K/F}(K_{S'}) \cap \mathfrak{D}_{F,S'}^*}{N_{K/F}(\mathfrak{D}_{K,S'}^*)} \end{aligned}$$

where $K_{S'} := \{\beta \in K^* \mid \nu_{\mathfrak{P}}(\beta^{\sigma-1}) \equiv 0 \pmod{3} \text{ for any } \mathfrak{P} \in \mathcal{P}_{K,S'}\}$.

Furthermore if $\text{Cl}_{K,S'}$ is G -invariant then $\mathcal{X}_H(F)/\widehat{\phi}(\widehat{\mathcal{X}_H}(F)) \hookrightarrow {}_N\mathfrak{U}_{K,S'} \oplus \mu_3(F)$.

Theorem 5.3. *Let F be a number field of class number 1 in which 3 splits completely. For a cyclic cubic extension K/F , let $\{1, \alpha, \alpha^2\}$ be a F -basis of K that \mathcal{X} is defined by the polynomial (1.1) with. Here $\alpha \in K$ denotes a root of the generic polynomial $\mathfrak{g}(x; t)$ in §8 for some $t \in F$. Let H be the hyperplane $z = 0$. Assume $t \in \mathfrak{D}_F$, $\delta(\mathfrak{g}) \notin F_{\mathfrak{p}}^{*3}$ for each $\mathfrak{p} \mid 3$. Then the set S in Lemma 5.1 consists of all the finite primes of F which ramifies in K and*

$$\begin{aligned} \dim_{\mathbb{F}_3} S^{(\hat{\phi})}(\mathcal{X}_H/F) + \text{rank}_{\mathbb{Z}} \mathfrak{D}_F^* &= \dim_{\mathbb{F}_3} S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/F) = \dim_{\mathbb{F}_3} {}_N\Phi_{F,S}, \\ 1 &\leq \text{rank}_{\mathbb{Z}} \mathcal{X}_H(F) \leq 2 \dim_{\mathbb{F}_3} {}_N\Phi_{F,S} - \text{rank}_{\mathbb{Z}} \mathfrak{D}_F^* - 1. \end{aligned}$$

Combining Proposition 4.1 with Theorem 1.3 and 5.3 yields a certain description for ${}_N\text{Cl}_K^G[3]$.

Corollary 5.4. *Under the first assumption in Theorem 1.3, there is the equality*

$$\begin{aligned} 3 \cdot \# {}_N\text{Cl}_K^G[3] &= 2 \cdot \# \left\{ L \in \mathfrak{Gal}(C_3/\mathbb{Q}) \mid \begin{array}{l} L/\mathbb{Q} \text{ is unramified outside } S_0 \\ L \cdot \mathbb{Q}_p \in \text{Im } \delta_{\mathbb{Q}_p} \text{ for any } p \in S_0 \end{array} \right\} - 1 \\ &= \# {}_N\Phi_{\mathbb{Q},S} \end{aligned}$$

where S is the set of all the finite primes of F which ramifies in K and the other notation is the same as in Proposition 4.1.

Example 5.5. Here we give an example for ${}_N\text{Cl}_K^G[3]$ being non-trivial in the case $F = \mathbb{Q}$. Let $t = -3^3$. Then the conductor of the minimal splitting field of $\mathfrak{g}(x; t)$ is $657 = 3^2 \cdot 73$, and the class number is 9 (see [6]). Since both 3, 73 lies in the image of the norm map, Using Corollary 5.4 yields ${}_N\text{Cl}_K^G[3] \simeq \mathbb{Z}/3\mathbb{Z}$. This example also satisfy $\delta(\mathfrak{g}) = 657 \notin \mathbb{Q}_3^{*3}$ (cf. Theorem 1.3).

The rest of this section is devoted to the proof of the above theorems. First of all, in view of Lemma 4.3, 5.1, we shall introduce finite groups for the sets S, S' in Lemma 5.1 defined by

$${}_N\mathfrak{R}_{F,S} := \left\{ \bar{d} \in \mathfrak{R}_{F,S} \mid d \in N_{K/F}(K^*) \right\}, \quad {}_N\mathfrak{R}_{K,S'} := \left\{ \bar{\alpha} \in \mathfrak{R}_{K,S'} \mid N_{K/F}(\alpha) = 1 \right\}.$$

From Lemma 7.3, the G -invariant subgroup ${}_N\mathfrak{R}_{K,S'}^G$ may be written by

$${}_N\mathfrak{R}_{K,S'}^G = \left\{ \bar{d} \in \mu_3(F)N_{K/F}(K^*)K^{*3}/K^{*3} \mid \nu_{\mathfrak{P}}(d) \equiv 0 \pmod{3} \text{ for any } \mathfrak{P} \in \mathcal{P}_{K,S'} \right\}.$$

When $\zeta_3 \in F$, the cyclic cubic extension K is generated over F by $\sqrt[3]{D}$ for some $D \in F^* \setminus F^{*3}$ from Kummer theory, which implies $D = N_{K/F}(\sqrt[3]{D})$ and $\nu_{\mathfrak{P}}(D) \equiv 0 \pmod{3}$ for any $\mathfrak{P} \in \mathcal{P}_K$ since each prime $\mathfrak{p} \in \mathcal{P}_F$ with $3 \nmid \nu_{\mathfrak{p}}(D)$ ramifies in K . Combining this with Lemma 7.1 yields

$$\begin{aligned} {}_N\mathfrak{R}_{K,S'}^G \oplus (F^* \cap K^{*3})/F^{*3} &\simeq \left\{ \bar{d} \in \mu_3(F)N_{K/F}(K^*)/F^{*3} \mid \nu_{\mathfrak{P}}(d) \equiv 0 \pmod{3} \text{ for any } \mathfrak{P} \in \mathcal{P}_{K,S'} \right\} \\ &\simeq \left\{ \bar{d} \in N_{K/F}(K^*)/F^{*3} \mid \nu_{\mathfrak{P}}(d) \equiv 0 \pmod{3} \text{ for any } \mathfrak{P} \in \mathcal{P}_{K,S'} \right\} \oplus \overline{\mu_3}(F) \\ &= \left\{ \bar{d} \in N_{K/F}(K^*)/F^{*3} \mid \nu_{\mathfrak{p}}(d) \equiv 0 \pmod{3} \text{ for any } \mathfrak{p} \in \mathcal{P}_{F,S \cup R} \right\} \oplus \overline{\mu_3}(F) \end{aligned}$$

where $\overline{\mu_3}(F) := \frac{\mu_3(F)N_{K/F}(K^*)}{N_{K/F}(K^*)}$ and R stands for the set of all the finite primes of F which ramifies in K . We understand \oplus as the direct sum of \mathbb{F}_3 -vector spaces. The last equality follows from the definition of S, S' . It thus turns out that ${}_N\mathfrak{R}_{F,S} \oplus \overline{\mu_3}(F) \hookrightarrow {}_N\mathfrak{R}_{K,S'}^G \oplus (F^* \cap K^{*3})/F^{*3}$. Then these groups contain the $\widehat{\phi}$ -Selmer group as follows.

Proposition 5.6. *There are inclusions as \mathbb{F}_3 -vector spaces:*

$$S^{(\widehat{\phi})}(\widehat{\mathcal{X}_H}/F) \oplus \overline{\mu_3}(F) \hookrightarrow {}_N\mathfrak{R}_{F,S} \oplus \overline{\mu_3}(F) \hookrightarrow {}_N\mathfrak{R}_{K,S'}^G \oplus (F^* \cap K^{*3})/F^{*3}.$$

Furthermore, if we assume the following conditions then all those groups coincide and $S = R, S' = \emptyset$. Let $v_{\mathfrak{p}} := \nu_{\mathfrak{p}}(N_{K/F}(\gamma(\mathcal{X}_H))) \in \mathbb{Z}$ for $\mathfrak{p} \in \mathcal{P}_F$.

- ◇ 3 splits completely in F ,
- ◇ The hyperplane is $H : z = 0$,
- ◇ Each finite prime $\mathfrak{p} \in \mathcal{P}_F$ satisfying $3 \nmid v_{\mathfrak{p}}$ ramifies in K ,
- ◇ For each $\mathfrak{p} \mid 3$, if $3 \mid v_{\mathfrak{p}}$ then \mathfrak{p} is unramified in K and $N_{K/F}(\gamma(\mathcal{X}_H)) \notin F_{\mathfrak{p}}^{*3}$.

Proof. Using Lemma 4.3 and 5.1 yields $S^{(\widehat{\phi})}(\widehat{\mathcal{X}_H}/F) \subset {}_N\mathfrak{R}_{F,S}$. Now we shall prove the latter statement. Since $H : z = 0$, a direct calculation shows us $N_{K/F}(\gamma(\mathcal{X}_H)) = -N_{K/F}(\alpha_1 - \alpha_1^{\sigma})$ where $\{1, \alpha_1, \alpha_2\}$ denotes the F -basis of K for \mathcal{X} . It thus follows from Lemma 7.5 that $S = R, S' = \emptyset$ under the conditions, and in particular ${}_N\mathfrak{R}_{F,S} \oplus \overline{\mu_3}(F) \simeq {}_N\mathfrak{R}_{K,S'}^G \oplus (F^* \cap K^{*3})/F^{*3}$. Finally we show the inclusion $S^{(\widehat{\phi})}(\widehat{\mathcal{X}_H}/F) \supset {}_N\mathfrak{R}_{F,S}$. Let \bar{d} be arbitrary element in ${}_N\mathfrak{R}_{F,S}$. For any $\mathfrak{p} \in \mathcal{P}_F$, the following chart can be verified from [9], Theorem 4.1.

$$\begin{cases} 3 \mid v_{\mathfrak{p}} \rightarrow \begin{cases} \mathfrak{p} \mid 3 \rightarrow \text{See below } \cdots (*) \\ \mathfrak{p} \nmid 3 \rightarrow \mathfrak{p} \in \mathcal{P}_{F,S} \text{ and hence } \bar{d} \in \text{Im } \widehat{\delta}_{F_{\mathfrak{p}}} = \mathfrak{D}_{F_{\mathfrak{p}}}^*/\mathfrak{D}_{F_{\mathfrak{p}}}^{*3} \end{cases} \\ 3 \nmid v_{\mathfrak{p}} \rightarrow \text{From Lemma 7.7, } \bar{d} \in \text{Im } \widehat{\delta}_{F_{\mathfrak{p}}} = N_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}(K_{\mathfrak{p}}^*)/F_{\mathfrak{p}}^{*3} \end{cases}$$

We consider the lack of the above chart indicated (*). By using the equivalence and the notation in Remark 4.6, the condition $3 \mid v_{\mathfrak{p}}, N_{K/F}(\gamma(\mathcal{X}_H)) \notin F_{\mathfrak{p}}^{*3}$ can be read into $u_{\pi} \not\equiv k_{\pi}^3 \pmod{9}$. Here we may choose 3 as a prime element $\pi \in F_{\mathfrak{p}}$. Let $\mathcal{D}' := u_{\pi}(u_{\pi} + \frac{u_{\pi} - k_{\pi}^3}{3})$. Since $u_{\pi} \equiv \pm 1 \pmod{3}$ from the condition 3 splits completely in F , it can be verified that $u_{\pi} \not\equiv k_{\pi}^3 \pmod{9}$ if and only if $(\frac{\mathcal{D}'}{\mathfrak{p}}) \neq 1$, which denotes the Legendre symbol. From [9], Theorem 4.1, this implies $\bar{d} \in \text{Im } \widehat{\delta}_{F_{\mathfrak{p}}}$. Consequently, we have $\bar{d} \in S^{(\widehat{\phi})}(\widehat{\mathcal{X}_H}/F)$. This completes the proof. \square

Remark 5.7. We consider the assumption in the above proposition more explicitly. Let $\alpha \in \overline{F}$ be a root of the generic polynomial $\mathfrak{g}(x; t)$ (see §8) with a fixed $t \in F$ so as to be $K = F(\alpha)$. We choose $\{1, \alpha, \alpha^2\}$ as the F -basis of K for \mathcal{X} . For any $\mathfrak{p} \in \mathcal{P}_F$ with $\nu_{\mathfrak{p}}(t) < 0$ we assume $3 \mid \nu_{\mathfrak{p}}(t)$. Let H be the hyperplane $z = 0$. Then $\pm N_{K/F}(\gamma(\mathcal{X}_H)) = \delta(\mathfrak{g}) = t^2 + 3t + 9$ satisfies the third condition by Proposition 8.1. Under the assumption that 3 splits completely in F , we can describe the condition $3 \mid v_{\mathfrak{p}}, \delta(\mathfrak{g}) \notin F_{\mathfrak{p}}^{*3}$ for $\mathfrak{p} \mid 3$ which is equivalent to $u_{\pi} \not\equiv k_{\pi}^3 \pmod{9}$ by using words of t as follows. (By Proposition 8.1, the condition implies that \mathfrak{p} is unramified in K .)

$$\begin{cases} \nu_{\mathfrak{p}}(t) < 0 & \rightarrow v_{\mathfrak{p}} = 2\nu_{\mathfrak{p}}(t) \rightarrow \text{The condition is equal to } 3^{-\nu_{\mathfrak{p}}(t)}t \equiv \pm 2, \pm 4 \pmod{9}. \\ \nu_{\mathfrak{p}}(t) = 0 & \rightarrow v_{\mathfrak{p}} = 0 \rightarrow \text{The condition is equal to } t \equiv 1, 5, 7, 8 \pmod{9}. \\ t \equiv 0, 6 \pmod{9} \rightarrow v_{\mathfrak{p}} = 2 & \rightarrow \text{This does not conform to } 3 \mid v_{\mathfrak{p}}, \text{ which is ignored.} \\ t \equiv 3 \pmod{9} \rightarrow v_{\mathfrak{p}} = 3 & \rightarrow \text{The condition is equal to } t \equiv 12 \pmod{27}. \end{cases}$$

This is often convenient for an explicit calculation.

The group $\mathfrak{R}_{F,S}$ relates to the 3-torsion subgroup of the S -ideal class group $\text{Cl}_{F,S}$ and the group of S -units $\mathfrak{O}_{F,S}^*$. There is an exact sequence

$$0 \longrightarrow \mathfrak{O}_{F,S}^* F^{*3} / F^{*3} \longrightarrow \mathfrak{R}_{F,S} \longrightarrow \text{Cl}_{F,S}[3] \longrightarrow 0$$

which is induced by the surjective homomorphism

$$\begin{aligned} \mathfrak{R}_{F,S} &\longrightarrow \text{Cl}_{F,S}[3] \\ \bar{d} &\longmapsto \overline{\prod_{\mathfrak{p} \in \mathcal{P}_{F,S}} \mathfrak{p}^{\nu_{\mathfrak{p}}(d)/3} \mathfrak{O}_{F,S}}. \end{aligned}$$

Since ${}_N\mathfrak{R}_{F,S}$ is a subgroup of $\mathfrak{R}_{F,S}$, one can obtain a restricted map from ${}_N\mathfrak{R}_{F,S}$ to $\text{Cl}_{F,S}[3]$. According to this, we would like to restrict the group $\text{Cl}_{F,S}[3]$ so as to hold the surjectivity of this map. This is the reason why we introduced the subgroup ${}_N\text{Cl}_{F,S}[3]$. It is easily verified that the group ${}_N\text{Cl}_{F,S}[3]$ is the exact image of ${}_N\mathfrak{R}_{F,S}$. We thus obtain the exact sequence

$$(5.1) \quad 0 \longrightarrow {}_N\Phi_{F,S} \longrightarrow {}_N\mathfrak{R}_{F,S} \longrightarrow {}_N\text{Cl}_{F,S}[3] \longrightarrow 0$$

where ${}_N\Phi_{F,S} = \{\bar{d} \in \mathfrak{O}_{F,S}^* F^{*3} / F^{*3} \mid d \in F^*, d \in N_{K/F}(K^*)\}$ is the kernel of the map.

Similarly, the group $\mathfrak{R}_{K,S'}$ also relates to the 3-torsion subgroup of the S' -ideal class group $\text{Cl}_{K,S'}$ and the group of S' -units $\mathfrak{O}_{K,S'}^*$. The restriction to the subgroup

${}_N\mathfrak{R}_{K,S'}$ of the surjective homomorphism as G -modules

$$\begin{aligned} \mathfrak{R}_{K,S'} &\longrightarrow \text{Cl}_{K,S'}[3] \\ \bar{\alpha} &\longmapsto \overline{\prod_{\mathfrak{P} \in \mathcal{P}_{K,S'}} \mathfrak{P}^{\nu_{\mathfrak{P}}(\alpha)/3} \mathfrak{D}_{K,S'}} \end{aligned}$$

induces the exact sequence

$$0 \longrightarrow \Psi \longrightarrow {}_N\mathfrak{R}_{K,S'} \longrightarrow {}_N\text{Cl}_{K,S'}[3] \longrightarrow 0$$

with the kernel $\Psi := \{\bar{\alpha} \in \mathfrak{D}_{K,S'}^* K^{*3}/K^{*3} \mid \alpha \in K^*, N_{K/F}(\alpha) = 1\}$, which can be rewritten as

$$\Psi = \left\{ \bar{\epsilon} \in \mathfrak{D}_{K,S'}^* K^{*3}/K^{*3} \mid \epsilon \in \mathfrak{D}_{K,S'}^*, N_{K/F}(\epsilon) \in N_{K/F}(K^{*3}) \right\}.$$

Taking Galois cohomology yields the long exact sequence

$$0 \longrightarrow \Psi^G \longrightarrow {}_N\mathfrak{R}_{K,S'}^G \longrightarrow {}_N\text{Cl}_{K,S'}^G[3] \longrightarrow H^1(K/F, \Psi) \longrightarrow H^1(K/F, {}_N\mathfrak{R}_{K,S'}) \longrightarrow \cdots.$$

We can describe the image of ${}_N\text{Cl}_{K,S'}^G[3]$ in $H^1(K/F, \Psi)$ as follows.

Proposition 5.8. *The following sequence is exact.*

$$0 \longrightarrow \Psi^G \longrightarrow {}_N\mathfrak{R}_{K,S'}^G \longrightarrow {}_N\text{Cl}_{K,S'}^G[3] \longrightarrow \frac{N_{K/F}(K_{S'}) \cap \mathfrak{D}_{F,S'}^*}{N_{K/F}(\mathfrak{D}_{K,S'}^*)} \longrightarrow 0.$$

Here $K_{S'} := \{\beta \in K^* \mid \nu_{\mathfrak{P}}(\beta^{\sigma-1}) \equiv 0 \pmod{3} \text{ for any } \mathfrak{P} \in \mathcal{P}_{K,S'}\}$.

Proof. We have only to prove the following map is surjective with the kernel $N_{K/F}(\mathfrak{D}_{K,S'}^*)$.

$$\begin{aligned} N_{K/F}(K_{S'}) \cap \mathfrak{D}_{F,S'}^* &\longrightarrow \text{Ker} [H^1(K/F, \Psi) \rightarrow H^1(K/F, {}_N\mathfrak{R}_{K,S'})] \\ N_{K/F}(\beta) &\longmapsto \bar{\xi} \end{aligned}$$

where ξ denotes a cocycle determined by letting $\xi_{\sigma} := \overline{N_{K/F}(\beta)}$. First of all, we show the map is well-defined. If so, this is a homomorphism by definition. Let $N_{K/F}(\beta)$ be arbitrary element in $N_{K/F}(K_{S'}) \cap \mathfrak{D}_{F,S'}^*$. Then $N_{K/F}(\beta) = (\beta^{\sigma-1})^{\sigma-1} \beta^{3\sigma} \in \mathfrak{D}_{F,S'}^*$, and $N_{K/F}(N_{K/F}(\beta)) = N_{K/F}(\beta^3) \in N_{K/F}(K^{*3})$, therefore $\overline{N_{K/F}(\beta)} \in \Psi$. Moreover, $\overline{\beta^{\sigma-1}} \in {}_N\mathfrak{R}_{K,S'}$ since $\beta \in K_{S'}$. These imply that $\bar{\xi}$ lies in the right-hand side.

[Kernel] Assume the image $\bar{\xi}$ of $N_{K/F}(\beta) \in N_{K/F}(K_{S'}) \cap \mathfrak{D}_{F,S'}^*$ is trivial, namely $\xi_{\sigma} = \overline{N_{K/F}(\beta)} = \overline{\epsilon^{\sigma-1}}$ for some $\epsilon \in \mathfrak{D}_{K,S'}^*$. Then there is some $\epsilon_0 \in \mathfrak{D}_{K,S'}^*$ so that $N_{K/F}(\beta) = \epsilon^{\sigma-1} \epsilon_0^3$ and hence $N_{K/F}(\beta) \in N_{K/F}(\mathfrak{D}_{K,S'}^*)$ by Lemma 7.2. Conversely, for any $N_{K/F}(\epsilon) \in N_{K/F}(\mathfrak{D}_{K,S'}^*)$, we find that $\overline{N_{K/F}(\epsilon)} = \overline{(\epsilon^{\sigma-1})^{\sigma-1}}$ corresponds to a coboundary class in $H^1(K/F, \Psi)$. Thus the kernel is $N_{K/F}(\mathfrak{D}_{K,S'}^*)$.

[Surjectivity] Let $\bar{\xi}$ be any element in the right-hand side. This can be written as $\xi_{\sigma} = \overline{\alpha^{\sigma-1}} \in \Psi$ with $\bar{\alpha} \in {}_N\mathfrak{R}_{K,S'}$, $N_{K/F}(\alpha) = 1$ by definition. From this, we observe $\epsilon := \alpha^{\sigma-1} \beta^3 \in \mathfrak{D}_{K,S'}^*$ for some $\beta \in K^*$, and $\epsilon^{\sigma-1} = (\alpha^{-\sigma} \beta^{\sigma-1})^3 \in \mathfrak{D}_{K,S'}^{*3}$. These imply $N_{K/F}(\beta)^3 = N_{K/F}(\epsilon) \in \mathfrak{D}_{F,S'}^*$ and $\beta \in K_{S'}$, namely $N_{K/F}(\beta) \in N_{K/F}(K_{S'}) \cap \mathfrak{D}_{F,S'}^*$. We claim that this $N_{K/F}(\beta)$ is mapped to $\bar{\xi}$. Since $\epsilon = N_{K/F}(\beta)(\alpha^{-\sigma} \beta^{\sigma-1})^{\sigma^2-1}$, it is seen that $\overline{N_{K/F}(\beta)}$ is equivalent to $\overline{\alpha^{\sigma-1}}$ modulo Ψ^{σ^2-1} , which implies the image of $N_{K/F}(\beta)$ is $\bar{\xi}$. This completes the proof. \square

Remark 5.9. Assume $F = \mathbb{Q}$ and each prime \mathfrak{P} of K lying above any $p \in S'$ is principal. Since all the primes in S' split completely in K , there is a prime element $\Pi \in \mathfrak{D}_{K,S'}^*$ such that $p = N_{K/F}(\Pi) \in \mathfrak{D}_{\mathbb{Q},S'}^*$. We thus have $\mathfrak{D}_{\mathbb{Q},S'}^* = \mathbb{Z}^* \oplus \langle p \mid p \in S' \rangle \subset N_{K/\mathbb{Q}}(\mathfrak{D}_{K,S'}^*)$. In addition, $\text{Cl}_{K,S'} \simeq \text{Cl}_K / \langle \overline{\mathfrak{P}} \rangle_{\mathfrak{P} \mid p \in S'} \simeq \text{Cl}_K$ from the property of S' -ideal class groups. Applying these to Proposition 5.8 yields the short exact sequence

$$0 \longrightarrow \Psi^G \longrightarrow {}_N\mathfrak{R}_{K,S'}^G \longrightarrow {}_N\text{Cl}_K^G[3] \longrightarrow 0.$$

Lemma 5.10. $\Psi^G \simeq {}_N\mathfrak{U}_{K,S'} \oplus \overline{\mu}_3(F)$.

Proof. First, for any $\overline{\alpha^{\sigma-1}} \in {}_N\mathfrak{U}_{K,S'}$ it is seen that $(\alpha^{\sigma-1})^{\sigma-1} = N_{K/F}(\alpha)\alpha^{-3\sigma} \in K^{*3}$ and $\mu_3(F)K^{*3}/K^{*3} \subset \Psi^G$. Thus the inclusion $\mu_3(F){}_N\mathfrak{U}_{K,S'} \subset \Psi^G$ holds. Conversely, for any $\overline{\alpha} \in \Psi^G$ we may assume $N_{K/F}(\alpha) = 1$. Since $\overline{\alpha}$ is G -invariant, there is some $\beta \in K^*$ so that $\alpha^{\sigma-1} = \beta^{-3}$, hence $N_{K/F}(\beta) = 1$ by using Lemma 7.2. From the equality $1 = \alpha^{1+\sigma+\sigma^2} = (\alpha^\sigma \beta^{1-\sigma})^3$, we have $r := \alpha^\sigma \beta^{1-\sigma} \in \mu_3(K) = \mu_3(F)$ and $\overline{\alpha} = \overline{r\beta^{\sigma-1}} \in \mu_3(F){}_N\mathfrak{U}_{K,S'}$, thus $\Psi^G \subset \mu_3(F){}_N\mathfrak{U}_{K,S'}$. Therefore $\Psi^G = \mu_3(F){}_N\mathfrak{U}_{K,S'}$. If $\mu_3(F) \subset N_{K/F}(K^*)$ then $\mu_3(F) \subset {}_N\mathfrak{U}_{K,S'}$ from Lemma 7.2, and hence $\Psi^G = {}_N\mathfrak{U}_{K,S'}$. Assume $\mu_3(F) \not\subset N_{K/F}(K^*)$, namely $\mu_3(F) = \langle \zeta_3 \rangle$ and $\mu_3(F) \cap N_{K/F}(K^*) = \{1\}$. We claim that the \mathbb{F}_3 -vector space $\mu_3(F){}_N\mathfrak{U}_{K,S'}$ is isomorphic to ${}_N\mathfrak{U}_{K,S'} \oplus \overline{\mu}_3(F)$, which is given by the map $\overline{r\beta^{\sigma-1}} \mapsto (\overline{\beta^{\sigma-1}}, \overline{r})$ where $r \in \mu_3(F)$, $\beta^{\sigma-1} \in {}_N\mathfrak{U}_{K,S'}$. If the map is well-defined then this is an injective homomorphism. The surjectivity is also clear. For any representative $r'\beta'^{\sigma-1} \in \overline{r\beta^{\sigma-1}}$, since $r'r^{-1}(\beta'\beta^{-1})^{\sigma-1} \in K^{*3}$ and $N_{K/F}(\beta'\beta^{-1}) = 1$, using Lemma 7.2 yields $r'r^{-1} \in \mu_3(F) \cap N_{K/F}(K^*)$. Consequently it must be $r' = r$ and $(\beta'\beta^{-1})^{\sigma-1} \in K^{*3}$. Therefore the map is well-defined. \square

Roughly speaking, the following lemma implies that the half of the Mordell-Weil group is bounded by a unit group.

Lemma 5.11. If $\text{Cl}_{K,S'}$ is G -invariant then $\mathcal{X}_H(F)/\widehat{\phi}(\widehat{\mathcal{X}_H(F)}) \hookrightarrow {}_N\mathfrak{U}_{K,S'} \oplus (F^* \cap K^{*3})/F^{*3}$.

Proof. It follows from Lemma 7.1 that $\text{Im } \widehat{\delta}_F \hookrightarrow \text{Im } \widehat{\delta}_F^K \oplus (F^* \cap K^{*3})/F^{*3}$. Now we shall prove the inclusion $\text{Im } \widehat{\delta}_F^K \hookrightarrow {}_N\mathfrak{U}_{K,S'}$. From Proposition 6.3, the image of $\widehat{\delta}_F^K$ can be written by $\frac{(x+y\alpha_1+z\alpha_2)^\sigma}{x+y\alpha_1+z\alpha_2} K^{*3}$. Let $\alpha := x + y\alpha_1 + z\alpha_2$ for short. Then $N_{K/F}(\alpha) = 1$ by the defining equation of \mathcal{X}_H . We must show that $\alpha^{\sigma-1}K^{*3}$ lies in $\mathfrak{D}_{K,S'}^*K^{*3}/K^{*3}$ under the assumption. For any $\mathfrak{P} \in \mathcal{P}_{K,S'}$, let $\mathfrak{p} := \mathfrak{P} \cap F$. if \mathfrak{p} is inert or ramifies in K then $\nu_{\mathfrak{p}}(\alpha^{\sigma-1}) = 0$. Assume \mathfrak{p} splits completely in K . The \mathfrak{p} -part of α may be written as $\mathfrak{P}^{v_0} \mathfrak{P}^{v_1\sigma} \mathfrak{P}^{v_2\sigma^2}$ with integers $v_0, v_1, v_2 \in \mathbb{Z}$. Since $\mathfrak{p} \in \mathcal{P}_{F,S'}$ and the \mathfrak{p} -part of $\alpha^{\sigma-1}$ is $\mathfrak{P}^{v_2-v_0} \mathfrak{P}^{(v_0-v_1)\sigma} \mathfrak{P}^{(v_1-v_2)\sigma^2}$, by using Lemma 5.1 there are some integers $r, r' \in \mathbb{Z}$ such that $v_0 - v_1 = 3r$, $v_1 - v_2 = 3r'$. It thus turns out that the \mathfrak{p} -part of $\alpha^{\sigma-1}$ is equal to $(\mathfrak{P}^{\sigma-1})^{3r} (\mathfrak{P}^{\sigma^2-1})^{3r'}$. Using the assumption $\text{Cl}_{K,S'}^G = \text{Cl}_{K,S'}$, there is some $\lambda_{\mathfrak{p}} \in K^*$ such that $\mathfrak{P}^{\sigma-1} \mathfrak{D}_{K,S'} = \lambda_{\mathfrak{p}} \mathfrak{D}_{K,S'}$, and hence the \mathfrak{p} -part is the principal ideal $(\lambda_{\mathfrak{p}}^{r+r'(\sigma+1)})^3 \mathfrak{D}_{K,S'}$. We can take such $\lambda_{\mathfrak{p}} \in K^*$ for each $\mathfrak{p} \in \mathcal{P}_{F,S'}$ so as to split completely in K , and let β^{-1} be a product of all $\lambda_{\mathfrak{p}}^{r+r'(\sigma+1)}$ which varies through those \mathfrak{p} , namely $\beta := \prod (\lambda_{\mathfrak{p}}^{r+r'(\sigma+1)})^{-1} \in K^*$. Here the integers r, r' are both 0 for almost all primes in $\mathcal{P}_{F,S'}$. Then $\alpha^{\sigma-1} \beta^3 \in \mathfrak{D}_{K,S'}^*$ by the definition. This yields the lemma. \square

We are now ready to prove the theorems.

Proof of Theorem 5.2. This is a direct consequence deduced from Proposition 5.6, 5.8 and Lemma 5.10, 5.11. \square

Proof of Theorem 5.3. Since $N_{K/F}(\gamma(\mathcal{X}_H)) = -\delta(\mathcal{X}) = \pm\delta(\mathfrak{g})$, under the assumption, a finite prime \mathfrak{p} of F ramifies in K if and only if $3 \nmid \nu_{\mathfrak{p}}(N_{K/F}(\gamma(\mathcal{X}_H)))$ by using Corollary 8.2. From Proposition 5.6 and the sequence (5.1), we have $S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/F) = {}_N\mathfrak{R}_K^G = {}_N\mathfrak{R}_{F,S} = {}_N\Phi_{F,S}$. Since $\zeta_3 \in F_{\mathfrak{p}}$ for \mathfrak{p} which ramifies tamely in K , applying Proposition 4.5 with the assumption $\delta(\mathcal{X}) \notin F_{\mathfrak{p}}^{*3}$ for $\mathfrak{p} \mid 3$ and Remark 7.8 yields $d_+ = 0$, $d_- - d_{\infty} = 0$ and hence the equality

$$(5.2) \quad \dim_{\mathbb{F}_3} S^{(\hat{\phi})}(\mathcal{X}_H/F) + \text{rank}_{\mathbb{Z}} \mathfrak{D}_F^* = \dim_{\mathbb{F}_3} S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/F).$$

The estimate $1 \leq \text{rank}_{\mathbb{Z}} \mathcal{X}_H(F) \leq 2 \dim_{\mathbb{F}_3} {}_N\Phi_{F,S} - \text{rank}_{\mathbb{Z}} \mathfrak{D}_F^* - 1$ now follows from the formula (4.1) with Lemma 7.10. \square

Proof of Theorem 1.3. The assumption is equivalent to that of Theorem 5.3 applied with $F = \mathbb{Q}$. The first statement follows from Remark 5.9, Lemma 5.10, 7.9, the equality (5.2) and the formula (4.1). Further assume Cl_K is G -invariant. Then Lemma 5.10, 5.11, 7.10 imply $\mathcal{X}_H(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{X}_H}(\mathbb{Q})) \simeq {}_N\mathfrak{U}_K \simeq \Psi^G \simeq \mathbb{Z}/3\mathbb{Z}$. Summarizing them with Proposition 5.8 and Remark 5.9, we have the following equivalence of exact sequences.

$$\begin{array}{ccccccc} 0 & \longrightarrow & {}_N\mathfrak{U}_K & \longrightarrow & {}_N\mathfrak{R}_K^G & \longrightarrow & {}_N\text{Cl}_K^G[3] \longrightarrow 0 \\ & & \parallel & & \parallel & & \parallel \\ 0 & \longrightarrow & \mathcal{X}_H(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{X}_H}(\mathbb{Q})) & \longrightarrow & S^{(\hat{\phi})}(\widehat{\mathcal{X}_H}/\mathbb{Q}) & \longrightarrow & \text{III}(\widehat{\mathcal{X}_H}/\mathbb{Q})[\hat{\phi}] \longrightarrow 0. \end{array}$$

This completes the proof. \square

6. Construction of the homomorphism $\widehat{\delta}_{F_{\bullet}}^{K_{\bullet}}$

This section is a key part to carry out our preceding descent procedure. We continue to use the previous notation. The idea is an interchange of the specified base point \mathcal{O} into another point on the elliptic curve \mathcal{X}_H . As a consequence, we obtain an available description for the image of the map $\widehat{\delta}_{F_{\bullet}}^{K_{\bullet}}$. We begin by taking such a point. From the equation defining \mathcal{X}_H , there are K -rational points on $\mathcal{X}_H \cap \{w = 0\}$ which consists of

$$\begin{aligned} \mathcal{O}' &= [c\alpha_1 - b\alpha_2, a\alpha_2 - c, -a\alpha_1 + b, 0], \\ T' &:= [c\alpha_1^{\sigma} - b\alpha_2^{\sigma}, a\alpha_2^{\sigma} - c, -a\alpha_1^{\sigma} + b, 0] (= \mathcal{O}'^{\sigma}), \\ T'^{\sigma} &= [c\alpha_1^{\sigma^2} - b\alpha_2^{\sigma^2}, a\alpha_2^{\sigma^2} - c, -a\alpha_1^{\sigma^2} + b, 0] (= \mathcal{O}'^{\sigma^2}). \end{aligned}$$

We adopt the point \mathcal{O}' as a new base point on the elliptic curve \mathcal{X}_H over K , and denote the new elliptic curve by $\mathcal{X}'_H := (\mathcal{X}_H, \mathcal{O}')$. Note that all the points $\mathcal{O}', T', T'^{\sigma}$ lie on the same line $H \cap \{w = 0\}$ and hence $T' + T'^{\sigma} = \mathcal{O}'$ where the symbol $+$ stands for the group law of \mathcal{X}'_H . The point T' turns out to be a 3-torsion element in the Mordell-Weil group $\mathcal{X}'_H(K)$ as a consequence of the following lemma.

Lemma 6.1. *A rational function $\eta \in K(\mathcal{X}_H)^*$ defined by*

$$\eta(x, y, z, w) = \frac{x + y\alpha_1^\sigma + z\alpha_2^\sigma}{x + y\alpha_1 + z\alpha_2}$$

has the divisor $3(T') - 3(\mathcal{O}')$.

Proof. It is easy to check that $x(P) + y(P)\alpha_1 + z(P)\alpha_2 = 0$ if and only if $P = \mathcal{O}'$. From this, the divisor of the rational function η has the form $n(T') - n(\mathcal{O}')$ with some positive integer n . In the next place, we calculate the order of $\eta \in K(\mathcal{X}_H)$ at the point \mathcal{O}' . The regular local ring $K[\mathcal{X}_H]_{\mathcal{O}'}$ at \mathcal{O}' is the localization of $K[\mathcal{X}_H]$ with respect to the maximal ideal

$$((a\alpha_2 - c)x - (c\alpha_1 - b\alpha_2)y, (-a\alpha_1 + b)y - (a\alpha_2 - c)z, (c\alpha_1 - b\alpha_2)z - (-a\alpha_1 + b)x, w),$$

which turns out to be $(x + y\alpha_1 + z\alpha_2, w) = (w)$ by using the defining equation of \mathcal{X}_H . Therefore the function w defines a uniformizer in $K[\mathcal{X}_H]_{\mathcal{O}'}$. This yields $\text{ord}_{\mathcal{O}'}(\eta) = -3$ by using the defining equation of \mathcal{X}_H once again. Therefore n must be equal to 3 and we find T' is a 3-torsion point on \mathcal{X}'_H by the well-known Abel-Jacobi theorem. \square

Let $\tau : \mathcal{X}_H \rightarrow \mathcal{X}'_H$ be a translation map over K defined by $P \mapsto P + \mathcal{O}'$. Then $\tau(T) = T'$ and the composed maps $\phi \circ \tau^{-1} : \mathcal{X}'_H \rightarrow \widehat{\mathcal{X}_H}$, $\tau \circ \widehat{\phi} : \widehat{\mathcal{X}_H} \rightarrow \mathcal{X}'_H$ are 3-isogenies defined over K since these maps send a base point to a base point.

The Weil pairing plays an important role for constructing a homomorphism from a Mordell-Weil group to a quotient multiplicative group of the ground field. The constructed map is compatible with connecting homomorphisms of Galois cohomology and can be always described by a rational function f_P on \mathcal{X}_H if ever the support of the divisor of f_P is $\{P, \mathcal{O}'\}$ where $P \neq \mathcal{O}'$ is some torsion point defined over the ground field. As for details, we refer to [11]. We now apply these to our case.

By the notation K_\bullet/F_\bullet , we shall indicate the cyclic cubic extension K/F or an extension $K_{\mathfrak{p}}/F_{\mathfrak{p}}$ of local fields. The Weil pairing leads to the composed injection

$$\widehat{\delta}' : \mathcal{X}'_H(K_\bullet)/\tau \circ \widehat{\phi}(\widehat{\mathcal{X}_H}(K_\bullet)) \longrightarrow H^1(K_\bullet, \widehat{\mathcal{X}_H}[\widehat{\phi}]) \xrightarrow{e_{\tau \circ \widehat{\phi}}(\cdot, T')} H^1(K_\bullet, \mu_3) \longrightarrow K_\bullet^*/K_\bullet^{*3}$$

which maps an element P to $f_{T'}(P)K_\bullet^{*3}$ for any $P \in \mathcal{X}'_H(K_\bullet) \setminus \{\mathcal{O}', T'\}$. Here $f_{T'}$ is a rational function on \mathcal{X}'_H satisfying

$$\text{div}(f_{T'}) = 3(T') - 3(\mathcal{O}'), \quad f_{T'} \circ \tau \circ \widehat{\phi} = g_{T'}^3 \text{ for some } g_{T'} \in K(\widehat{\mathcal{X}_H}).$$

By the Abel-Jacobi theorem, such functions $f_{T'} \in K(\mathcal{X}'_H)$, $g_{T'} \in K(\widehat{\mathcal{X}_H})$ always exist.

From Lemma 6.1, since $\text{div}(\eta) = 3(T') - 3(\mathcal{O}')$, there is an element $\lambda \in K^*$ so that $f_{T'} = \lambda \cdot \eta$. Thus the image of the composed map $\widehat{\delta}' \circ \tau : \mathcal{X}_H(K_\bullet)/\widehat{\phi}(\widehat{\mathcal{X}_H}(K_\bullet)) \rightarrow K_\bullet^*/K_\bullet^{*3}$ is calculated as

$$\begin{aligned} \widehat{\delta}' \circ \tau(P) &= \widehat{\delta}' \circ \tau(P - \mathcal{O}')(\widehat{\delta}' \circ \tau(-\mathcal{O}'))^{-1} \\ &= \widehat{\delta}'(P)\widehat{\delta}'(\mathcal{O})^{-1} \\ (6.1) \quad &= (\lambda \cdot \eta(P))(\lambda \cdot \eta(\mathcal{O}))^{-1}K_\bullet^{*3} \\ &= \eta(P)K_\bullet^{*3} \quad \text{for any } P \in \mathcal{X}_H(K_\bullet) \setminus \{\mathcal{O}', T'\}. \end{aligned}$$

It is easily seen that $\widehat{\delta}' \circ \tau = \widehat{\delta}_{K_\bullet}$ by the equality $e_{\tau \circ \widehat{\phi}}(P, T') = e_{\widehat{\phi}}(P, T)$ for any $P \in \widehat{\mathcal{X}_H}[\widehat{\phi}]$.

Though we does not need to clarify the constant $\lambda \in K^*$ so far, it will be required to prove the proposition below. We next give the description for λ .

Lemma 6.2. $\lambda K^{*3} = \frac{\gamma(\mathcal{X}_H)}{\gamma(\mathcal{X}_H)^{\sigma^2}} K^{*3}$.

Proof. From the paper [9], §3, there is a homomorphism $\widehat{\delta}_{\mathcal{W}} : \mathcal{W}(\mathcal{X}_H)(K) \rightarrow K^*/K^{*3}$ which sends the point $\vartheta(T) = (0, 0)$ to $N_{K/F}(\gamma(\mathcal{X}_H))^{-1} K^{*3}$. Taking account of the Weil pairing with $\tau(T) = T'$, $\vartheta(T) = (0, 0)$ yields $\widehat{\delta}' \circ \tau = \widehat{\delta}_{\mathcal{W}} \circ \vartheta$. On the other hand, $\widehat{\delta}' \circ \tau(T) = \widehat{\delta}'(T') = \widehat{\delta}'(T'^{\sigma})^{-1} = \lambda^{-1} \eta(T'^{\sigma})^{-1} K^{*3}$. Here we used the relation $T' + T'^{\sigma} = \mathcal{O}'$. Moreover it is directly verified that $\eta(T'^{\sigma}) = -\frac{\gamma(\mathcal{X}_H)^{\sigma}}{\gamma(\mathcal{X}_H)^{\sigma^2}}$. We thus have $N_{K/F}(\gamma(\mathcal{X}_H))^{-1} K^{*3} = \lambda^{-1} \eta(T'^{\sigma})^{-1} K^{*3}$, namely $\lambda K^{*3} = \frac{\gamma(\mathcal{X}_H)}{\gamma(\mathcal{X}_H)^{\sigma^2}} K^{*3}$. \square

Summarizing the above arguments yields the following proposition.

Proposition 6.3. *The rational function $\eta \in K(\mathcal{X}_H)^*$ in Lemma 6.1 describes the map*

$$\begin{aligned} \widehat{\delta}_{F_\bullet}^{K_\bullet} : \mathcal{X}_H(F_\bullet)/\widehat{\phi}(\widehat{\mathcal{X}_H}(F_\bullet)) &\longrightarrow K_\bullet^*/K_\bullet^{*3} \\ [x, y, z, w] &\longmapsto \frac{x + y\alpha_1^\sigma + z\alpha_2^\sigma}{x + y\alpha_1 + z\alpha_2} K_\bullet^{*3}, \\ \mathcal{O}' &\longmapsto \frac{\gamma(\mathcal{X}_H)^{\sigma^2}}{\gamma(\mathcal{X}_H)} K_\bullet^{*3}, \\ T' &\longmapsto \frac{\gamma(\mathcal{X}_H)}{\gamma(\mathcal{X}_H)^\sigma} K_\bullet^{*3}. \end{aligned}$$

This homomorphism is injective if $\zeta_3 \notin F_\bullet$ or $F_\bullet = K_\bullet$.

Proof. There is the commutative diagram

$$\begin{array}{ccc} \mathcal{X}_H(F_\bullet)/\widehat{\phi}(\widehat{\mathcal{X}_H}(F_\bullet)) & \xrightarrow{\widehat{\delta}_{F_\bullet}} & F_\bullet^*/F_\bullet^{*3} \\ \downarrow & & \downarrow \\ \mathcal{X}_H(K_\bullet)/\widehat{\phi}(\widehat{\mathcal{X}_H}(K_\bullet)) & \xrightarrow{\widehat{\delta}_{K_\bullet}} & K_\bullet^*/K_\bullet^{*3}. \end{array}$$

Here $\widehat{\delta}_{F_\bullet}, \widehat{\delta}_{K_\bullet}$ are injections and the vertical arrows are natural maps. For any $P \in \mathcal{X}_H(F_\bullet) \setminus \{\mathcal{O}', T'\}$, we have $\widehat{\delta}_{F_\bullet}^{K_\bullet}(P) = \widehat{\delta}_{K_\bullet}(P) = \widehat{\delta}' \circ \tau(P) = \eta(P) K_\bullet^{*3}$ by (6.1). If $P = \mathcal{O}'$ then we can calculate as $\widehat{\delta}_{F_\bullet}^{K_\bullet}(\mathcal{O}') = (\widehat{\delta}' \circ \tau(-\mathcal{O}'))^{-1} = \widehat{\delta}'(\mathcal{O})^{-1} = \lambda^{-1} K_\bullet^{*3} = \frac{\gamma(\mathcal{X}_H)^{\sigma^2}}{\gamma(\mathcal{X}_H)} K_\bullet^{*3}$ by Lemma 6.2. Similarly, we have $\widehat{\delta}_{F_\bullet}^{K_\bullet}(T') = \frac{\gamma(\mathcal{X}_H)}{\gamma(\mathcal{X}_H)^\sigma} K_\bullet^{*3}$. The remaining statement follows from Lemma 7.1. \square

7. Local calculations and some lemmas

In this section we assemble some lemmas frequently used in the preceding sections.

Lemma 7.1. *We denote by K_\bullet/F_\bullet either K/F or $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ for finite primes $\mathfrak{P}/\mathfrak{p}$. The natural homomorphism $F_\bullet^*/F_\bullet^{*3} \rightarrow K_\bullet^*/K_\bullet^{*3}$ induced by the inclusion $F_\bullet \subset K_\bullet$ is injective if and only if $\zeta_3 \notin F_\bullet$ or $F_\bullet = K_\bullet$. More precisely, for an extension K_\bullet/F_\bullet the kernel of the natural homomorphism is*

$$(F_\bullet^* \cap K_\bullet^{*3})/F_\bullet^{*3} = \begin{cases} \langle DF_\bullet^{*3} \rangle & \text{if } \zeta_3 \in F_\bullet, \\ \{F_\bullet^{*3}\} & \text{if } \zeta_3 \notin F_\bullet, \end{cases}$$

$$(F_{\mathfrak{p}}^* \cap K_{\mathfrak{p}}^{*3})/F_{\mathfrak{p}}^{*3} = \begin{cases} \langle D_{\mathfrak{p}}F_{\mathfrak{p}}^{*3} \rangle & \text{if } \zeta_3 \in F_{\mathfrak{p}} \text{ and } \mathfrak{p} \text{ does not split completely in } K, \\ \{F_{\mathfrak{p}}^{*3}\} & \text{otherwise,} \end{cases}$$

where D_\bullet stands for some element in $F_\bullet^* \setminus F_\bullet^{*3}$ satisfying $K_\bullet = F_\bullet(\sqrt[3]{D_\bullet})$. Note that if $\zeta_3 \in F_{\mathfrak{p}}$ and $F_{\mathfrak{p}} \neq K_{\mathfrak{p}}$ then $\langle D_{\mathfrak{p}}F_{\mathfrak{p}}^{*3} \rangle = N_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}(K_{\mathfrak{p}}^*)/F_{\mathfrak{p}}^{*3}$. Further if \mathfrak{p} ramifies tamely in K then automatically $\zeta_3 \in F_{\mathfrak{p}}$ and $\langle D_{\mathfrak{p}}F_{\mathfrak{p}}^{*3} \rangle = \langle \pi F_{\mathfrak{p}}^{*3} \rangle$ with some prime element $\pi \in F_{\mathfrak{p}}$.

Proof. There is equivalent exact sequences

$$\begin{array}{ccccccc} 0 & \longrightarrow & (F_\bullet^* \cap K_\bullet^{*3})/F_\bullet^{*3} & \longrightarrow & F_\bullet^*/F_\bullet^{*3} & \longrightarrow & K_\bullet^*/K_\bullet^{*3} \\ & & \parallel & & \parallel & & \parallel \\ 0 & \longrightarrow & H^1(K_\bullet/F_\bullet, \mu_3^{\text{Gal}(\overline{F_\bullet}/K_\bullet)}) & \xrightarrow{\text{inf}} & H^1(F_\bullet, \mu_3) & \xrightarrow{\text{res}} & H^1(K_\bullet, \mu_3). \end{array}$$

Since the degree $[K_\bullet : F_\bullet]$ must divide 3, the condition $\zeta_3 \notin F_\bullet$ is equivalent to $\zeta_3 \notin K_\bullet$. Hence the cohomology group $H^1(K_\bullet/F_\bullet, \mu_3^{\text{Gal}(\overline{F_\bullet}/K_\bullet)})$ vanishes when $\zeta_3 \notin F_\bullet$ or \mathfrak{p} splits completely in K . Otherwise $H^1(K_\bullet/F_\bullet, \mu_3^{\text{Gal}(\overline{F_\bullet}/K_\bullet)})$ is isomorphic to the group $\mathbb{Z}/3\mathbb{Z}$. This proves the first assertion. The latter follows from theory of local fields and Kummer. \square

Lemma 7.2. *Let K_\bullet/F_\bullet denote K/F or $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ for finite primes $\mathfrak{P}/\mathfrak{p}$ which does not split completely. For an element $d \in F_\bullet^*$, the following conditions are equivalent.*

- $\diamond d = \alpha^{\sigma-1}\beta^3$ with some $\alpha, \beta \in K_\bullet^*$ satisfying $N_{K_\bullet/F_\bullet}(\alpha) \in F_\bullet^{*3}$.
- $\diamond d = N_{K_\bullet/F_\bullet}(\beta)$.

Proof. Assume the first condition and let $N_{K_\bullet/F_\bullet}(\alpha) = d_0^3$ for some $d_0 \in F_\bullet^*$ where $\text{Gal}(K_\bullet/F_\bullet) \simeq \langle \sigma \rangle$. Then $1 = (\alpha^{\sigma-1})^{1-\sigma} \beta^{3(1-\sigma)} = r^3$. Here $r := d_0^{-1} \alpha^\sigma \beta^{1-\sigma} \in \mu_3(K_\bullet) = \mu_3(F_\bullet)$ since the extension degree $[K_\bullet : F_\bullet]$ is equal to 3. We thus have $1 = r^{\sigma^2-1} = \alpha^{1-\sigma} \beta^{-3} N_{K_\bullet/F_\bullet}(\beta)$, and hence $d = N_{K_\bullet/F_\bullet}(\beta)$. The converse is immediate from $d = N_{K_\bullet/F_\bullet}(\beta) = (\beta^{1-\sigma^2})^{\sigma-1} \beta^3$. \square

Lemma 7.3. $((\text{Ker } N_{K/F})K^{*3}/K^{*3})^G = \mu_3(F)N_{K/F}(K^*)K^{*3}/K^{*3}$.

Proof. Since each element in the right-hand side has a representative of the form $d = rN_{K/F}(\beta) \in F^*$ with $r \in \mu_3(F)$, $\beta \in K^*$, the element $d\beta^{-3} \in \text{Ker } N_{K/F}$ represents an element in the left-hand side. Conversely, let $\alpha \in \text{Ker } N_{K/F}$ represent an element

in the left-hand side. Then there is an element $\beta \in K^*$ such that $\alpha^{\sigma-1} = \beta^3$, which implies $N_{K/F}(\beta) = 1$ from Lemma 7.2. By using Hilbert's "Satz 90", the element β is of the form $\beta_0^{1-\sigma}$ with some $\beta_0 \in K^*$ and hence $(\alpha\beta_0^3)^\sigma = \alpha\beta_0^3 \in F^*$. Letting $d := \alpha\beta_0^3 \in F^*$, we have $d^3 = N_{K/F}(\beta_0)^3$. Therefore $\overline{\alpha} = \overline{d}$ lies in the right-hand side. \square

Lemma 7.4. *For any finite prime \mathfrak{p} of F which ramifies tamely in K , The image of the map $\widehat{\delta}_{F_{\mathfrak{p}}}^{K_{\mathfrak{p}}}$ is trivial. Especially $\text{Im } \widehat{\delta}_{F_{\mathfrak{p}}} \subset \langle \pi F_{\mathfrak{p}}^{*3} \rangle$ for some prime element $\pi \in F_{\mathfrak{p}}$.*

Proof. Since $K_{\mathfrak{p}}/F_{\mathfrak{p}}$ is a proper extension, there is no $F_{\mathfrak{p}}$ -rational point on $\mathcal{X}_H \cap \{w = 0\}$. For any point $P = [x, y, z, 1] \in \mathcal{X}_H(F_{\mathfrak{p}})$ it is seen from the equation defining \mathcal{X}_H that $\nu_{\mathfrak{p}}(x + y\alpha_1 + z\alpha_2) = \nu_{\mathfrak{p}}(x + y\alpha_1^\sigma + z\alpha_2^\sigma) = \nu_{\mathfrak{p}}(x + y\alpha_1^{\sigma^2} + z\alpha_2^{\sigma^2}) = 0$, and hence $\eta(P) \equiv 1 \pmod{\mathfrak{p}}$ where η has defined in Lemma 6.1. Therefore $\eta(P)$ lies in $K_{\mathfrak{p}}^{*3}$ by Hensel's Lemma, which implies the desired result from Proposition 6.3 and Lemma 7.1. \square

Lemma 7.5. *For arbitrary $\alpha \in K \setminus F$, if a finite prime \mathfrak{p} of F ramifies tamely in K then $3 \nmid \nu_{\mathfrak{p}}(N_{K/F}(\alpha - \alpha^\sigma))$.*

Proof. Let \mathcal{X} be a cubic surface defined by the polynomial (1.1) with the F -basis $\{1, \alpha, \alpha^2\}$ of K . Consider the elliptic curve \mathcal{X}_H/F for the hyperplane $H : z = 0$. Then it is verified that $N_{K/F}(\gamma(\mathcal{X}_H)) = -\delta(\mathcal{X}) = -N_{K/F}(\alpha - \alpha^\sigma)$. If $3 \mid \nu_{\mathfrak{p}}(N_{K/F}(\gamma(\mathcal{X}_H)))$ then $\text{Im } \widehat{\delta}_{F_{\mathfrak{p}}} = \mathfrak{O}_{F_{\mathfrak{p}}}^*/\mathfrak{O}_{F_{\mathfrak{p}}}^{*3}$ by using [9], Theorem 4.1, which is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ since $\zeta_3 \in F_{\mathfrak{p}}$ when \mathfrak{p} ramifies tamely. However this contradicts Lemma 7.4. Therefore we have the desired result. \square

Remark 7.6. The statement of Lemma 7.5 seems to separate from the arithmetic of elliptic curves. Nevertheless it can be proven via certain elliptic curves.

Lemma 7.7. *Let \mathfrak{p} be a finite prime of F which ramifies in K . Assume $3 \nmid \nu_{\mathfrak{p}}(N_{K/F}(\gamma(\mathcal{X}_H)))$. If \mathfrak{p} ramifies wildly then we also assume 3 splits completely in F . Then $\text{Im } \widehat{\delta}_{F_{\mathfrak{p}}} = N_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}(K_{\mathfrak{p}}^*)/F_{\mathfrak{p}}^{*3}$.*

Proof. Let \mathfrak{P} be a prime above \mathfrak{p} . First of all, it is a direct consequence from Lemma 4.3 that $\text{Im } \widehat{\delta}_{F_{\mathfrak{p}}} \hookrightarrow N_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}(K_{\mathfrak{p}}^*)/F_{\mathfrak{p}}^{*3}$. It thus suffices to prove $\sharp \text{Im } \widehat{\delta}_{F_{\mathfrak{p}}} = [N_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}(K_{\mathfrak{p}}^*) : F_{\mathfrak{p}}^{*3}]$. By using the equivalence $\text{Gal}(K_{\mathfrak{p}}/F_{\mathfrak{p}}) \simeq F_{\mathfrak{p}}^*/N_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}(K_{\mathfrak{p}}^*)$ from local class field theory, it turns out that $N_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}(K_{\mathfrak{p}}^*)/F_{\mathfrak{p}}^{*3} \subsetneq F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*3}$ whose group index is equal to 3 because \mathfrak{p} ramifies in K . Under the assumption, since $[F_{\mathfrak{p}}^* : F_{\mathfrak{p}}^{*3}] = 9$, it must be $[N_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}(K_{\mathfrak{p}}^*) : F_{\mathfrak{p}}^{*3}] = 3$. Applying [9], Theorem 4.1 yields the required result. \square

Remark 7.8. Under the assumption of Lemma 7.7, if \mathfrak{p} ramifies wildly in K then the case $\nu_{\mathfrak{p}}(N_{K/F}(\gamma(\mathcal{X}_H))) \equiv 1 \pmod{3}$ cannot occur because this implies $\text{Im } \widehat{\delta}_{F_{\mathfrak{p}}} = F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*3}$ by [9], Theorem 4.1, which is contradiction.

Lemma 7.9. *Assume $F = \mathbb{Q}$ then $N\mathfrak{U}_K \simeq (\mathfrak{O}_K^*/\mathfrak{O}_K^{*3})^G \simeq \mathbb{Z}/3\mathbb{Z}$.*

Proof. First, the inclusion $N\mathfrak{U}_K \hookrightarrow (\mathfrak{O}_K^*K^{*3}/K^{*3})^G = (\mathfrak{O}_K^*/\mathfrak{O}_K^{*3})^G$ follows from $(\alpha^{\sigma-1})^{\sigma-1} = N_{K/\mathbb{Q}}(\alpha)\alpha^{-3\sigma} \in K^{*3}$ for any $\alpha^{\sigma-1} \in N\mathfrak{U}_K$. Since K is a totally real cubic field over \mathbb{Q} , the unit group is of the form $\mathfrak{O}_K^* = \langle -1, \epsilon_1, \epsilon_2 \rangle$ with fundamental units ϵ_1, ϵ_2 , and then $\mathfrak{O}_K^*/\mathfrak{O}_K^{*3} \simeq (\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$. It suffices to prove that there is some $\epsilon \in \mathfrak{O}_K^*$ so

as to be $\bar{\epsilon} \notin (\mathfrak{D}_K^*/\mathfrak{D}_K^{*3})^G$. If this is proven, then $\epsilon^{\sigma-1} \notin \mathfrak{D}_K^{*3}$, $N_{K/\mathbb{Q}}(\pm\epsilon) = 1$ and hence $\epsilon^{\sigma-1}$ represents a non-trivial element in ${}_N\mathfrak{U}_K$ because $(\epsilon^{\sigma-1})^{\sigma-1} = N_{K/\mathbb{Q}}(\epsilon)\epsilon^{-3\sigma} \in \mathfrak{D}_K^{*3}$. Thus the lemma follows. The units $\epsilon_1^\sigma, \epsilon_2^\sigma$ can be written by the form $\pm\epsilon_1^r\epsilon_2^s, \pm\epsilon_1^{r'}\epsilon_2^{s'}$ with integers $r, s, r', s' \in \mathbb{Z}$, respectively. Then the equalities $\epsilon_1^{\sigma^3} = \epsilon_1, \epsilon_2^{\sigma^3} = \epsilon_2$ cause the following equations for r, s, r', s' .

$$\begin{aligned} r(r^2 + r's) + sr'(r + s') &= 1, & s(r^2 + r's) + ss'(r + s') &= 0, \\ rr'(r + s') + r'(r's + s'^2) &= 0, & sr'(r + s') + s'(r's + s'^2) &= 1. \end{aligned}$$

From this we obtain

$$(r, s, r', s') = \begin{cases} (r, -\frac{r^2+r+1}{r'}, r', -1-r) & \text{if } ss' \neq 0, \\ (-1, \pm 1, -s, 0) & \text{if } s \neq 0 \text{ and } s' = 0, \\ (1, 0, 0, 1) & \text{if } s = 0. \end{cases}$$

However the last case $s = 0$ is impossible since $\epsilon_1, \epsilon_2 \in K \setminus F$. Let $\epsilon := \epsilon_1$ if $3 \nmid s$, while $\epsilon := \epsilon_2$ if $3 \mid s$. Then ϵ is the required element as follows. Assume $3 \nmid s$ then $\epsilon_1^{\sigma-1} \notin \mathfrak{D}_K^{*3}$. When $3 \mid s$ and $s \neq 0$, it must be $r \equiv 1 \pmod{3}$ and hence $9 \nmid r^2 + r + 1$. This implies $3 \nmid r'$ because $s \in \mathbb{Z}$. We thus have $\epsilon_2^{\sigma-1} \notin \mathfrak{D}_K^{*3}$. \square

Lemma 7.10. *Let F be a number field of class number 1 in which 3 splits completely. For a cyclic cubic extension K/F , let $\{1, \alpha, \alpha^2\}$ be a F -basis of K that \mathcal{X} is defined by the polynomial (1.1) with. Here $\alpha \in K$ denotes a root of the generic polynomial $\mathfrak{g}(x; t)$ in §8 for some $t \in F$. Let H be the hyperplane $z = 0$. Assume $\delta(\mathfrak{g}) \notin F_{\mathfrak{p}}^{*3}$ for each $\mathfrak{p} \mid 3$. Then*

$$\mathbb{Z}/3\mathbb{Z} \hookrightarrow \mathcal{X}_H(F)/\widehat{\phi}(\widehat{\mathcal{X}_H(F)}), \quad (\mathbb{Z}/3\mathbb{Z})^{\oplus 2} \hookrightarrow \mathcal{X}_H(F)/3\mathcal{X}_H(F).$$

Especially $\text{rank}_{\mathbb{Z}} \mathcal{X}_H(F) \geq 1$ from the formula (4.1).

Proof. By Remark 4.2, the group $\widehat{\mathcal{X}_H(F)}/\phi(\mathcal{X}_H(F))$ contains $\mathbb{Z}/3\mathbb{Z}$ as subgroup. It suffices to show that $\mathcal{X}_H(F)/\widehat{\phi}(\widehat{\mathcal{X}_H(F)})$ also contains $\mathbb{Z}/3\mathbb{Z}$. Then the statement follows from the formula $\mathcal{X}_H(F)/3\mathcal{X}_H(F) \simeq \mathcal{X}_H(F)/\widehat{\phi}(\widehat{\mathcal{X}_H(F)}) \oplus \widehat{\mathcal{X}_H(F)}/\phi(\mathcal{X}_H(F))$ in §4. In the paper [9], §3, there is a homomorphism $\widehat{\delta}_{\mathcal{W}} : \mathcal{W}(\mathcal{X}_H)(F) \rightarrow F^*/F^{*3}$ which sends the 3-torsion point $(0, 0)$ to $N_{K/F}(\gamma(\mathcal{X}_H))^{-1}F^{*3} = \delta(\mathfrak{g})^{-1}F^{*3}$. We can easily verify the relation $\widehat{\delta}_F = \widehat{\delta}_{\mathcal{W}} \circ \vartheta$ by $\vartheta(T) = (0, 0)$. Hence the subgroup generated by $\widehat{\delta}_F(T)$ is equal to $\langle \delta(\mathfrak{g})F^{*3} \rangle$. Since there is no proper unramified extension over F , $\delta(\mathfrak{g})$ has at least one prime divisor \mathfrak{p} satisfying $3 \nmid \nu_{\mathfrak{p}}(\delta(\mathfrak{g}))$ from Corollary 8.2. Thus $\delta(\mathfrak{g})$ is not a perfect cube in F . This implies $\bar{T} \in \mathcal{X}_H(F)/\widehat{\phi}(\widehat{\mathcal{X}_H(F)})$ is a non-trivial element. Therefore the proof is now ended. \square

8. A generic polynomial for cyclic cubic extensions

For an explicit or systematic calculation, the notion of generic polynomials are often useful. Generic polynomial is a polynomial which parameterizes all Galois extensions with a Galois group isomorphic to some fixed finite group G . The existence of generic polynomials for a given finite group G is unsolved problem. But it is known in the case G is cyclic of order 3.

A generic polynomial for the cyclic group $C_3 \simeq \mathbb{Z}/3\mathbb{Z}$ over a number field F used in the paper is

$$\mathbf{g}(x; t) := x^3 + tx^2 - (t+3)x + 1 \quad (t \in F)$$

whose discriminant is $(t^2 + 3t + 9)^2$. Let $\delta(\mathbf{g}) := t^2 + 3t + 9$. If α is a root of \mathbf{g} then $\frac{1}{1-\alpha}$, $1 - \frac{1}{\alpha}$ are all the other roots. When α does not lie in F , the extension $K := F(\alpha)/F$ is always cyclic cubic. Then $\delta(\mathbf{g})$ is also written as

$$\delta(\mathbf{g}) = \pm \begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^\sigma & \alpha^{2\sigma} \\ 1 & \alpha^{\sigma^2} & \alpha^{2\sigma^2} \end{vmatrix} \quad (= \pm N_{K/F}(\alpha - \alpha^\sigma)).$$

Here $\text{Gal}(K/F) = \langle \sigma \rangle \simeq C_3$ and the sign \pm depends on the choice of a generator σ . From the property, for arbitrary cyclic cubic extension K over F , there is some $t \in F$ so that the minimal splitting field of $\mathbf{g}(x; t) \in F[x]$ is exactly K .

As for the conductor of a cyclic cubic extension K/F , we have the following proposition.

Proposition 8.1. *Assume 3 splits completely in F . For any finite prime \mathfrak{p} of F , the \mathfrak{p} -conductor $\mathfrak{f}_{\mathfrak{p}} = \mathfrak{p}^{n_{\mathfrak{p}}}$ of the cubic extension K/F is given by the following chart.*

$$\begin{aligned} \nu_{\mathfrak{p}}(\delta(\mathbf{g})) \leq 0 &\rightarrow n_{\mathfrak{p}} = 0, \\ \nu_{\mathfrak{p}}(\delta(\mathbf{g})) > 0 &\rightarrow \begin{cases} 3 \nmid \nu_{\mathfrak{p}}(\delta(\mathbf{g})) \rightarrow n_{\mathfrak{p}} = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid 3, \\ 2 & \text{if } \mathfrak{p} \mid 3, \end{cases} \\ 3 \mid \nu_{\mathfrak{p}}(\delta(\mathbf{g})) \rightarrow \begin{cases} \mathfrak{p} \nmid 3 \rightarrow n_{\mathfrak{p}} = 0, \\ \mathfrak{p} \mid 3 \rightarrow n_{\mathfrak{p}} = \begin{cases} 0 & \text{if } \delta(\mathbf{g}) \notin F_{\mathfrak{p}}^{*3}, \\ 2 & \text{if } \delta(\mathbf{g}) \in F_{\mathfrak{p}}^{*3}. \end{cases} \end{cases} \end{cases} \end{aligned}$$

Proof. The proof for the case $\nu_{\mathfrak{p}}(\delta(\mathbf{g})) \geq 0$, but except for the case $3 \mid \nu_{\mathfrak{p}}(\delta(\mathbf{g})) > 0$ with $\mathfrak{p} \mid 3$, can be done essentially by the same way as Washington's one in [14], which is hence omitted. We assume $-v := \nu_{\mathfrak{p}}(\delta(\mathbf{g})) < 0$ and let π be a prime element in $F_{\mathfrak{p}}$. Then the polynomial $\pi^{3v}\mathbf{g}(\pi^{-v}x; t)$ has integral coefficients and the polynomial modulo π has a simple root. Therefore the root lifts to some $\alpha \in \mathfrak{O}_{F_{\mathfrak{p}}}$ such that $\pi^{3v}\mathbf{g}(\pi^{-v}\alpha; t) = 0$ by Hensel's lemma. It thus turns out that all the roots of $\mathbf{g}(x; t)$ are $\{\pi^{-v}\alpha, \frac{1}{1-\pi^{-v}\alpha}, 1 - \frac{1}{\pi^{-v}\alpha}\} \subset F_{\mathfrak{p}}$. This implies that \mathfrak{p} splits completely. Finally in the case $3 \mid \nu_{\mathfrak{p}}(\delta(\mathbf{g})) > 0$ with $\mathfrak{p} \mid 3$, we must show that \mathfrak{p} ramifies wildly if and only if $\delta(\mathbf{g}) \in F_{\mathfrak{p}}^{*3}$. First, t must be of the form $9t' + 3$ with some $t' \in \mathfrak{O}_{F_{\mathfrak{p}}}$ by $3 \mid \nu_{\mathfrak{p}}(\delta(\mathbf{g})) > 0$. If $\delta(\mathbf{g}) \notin F_{\mathfrak{p}}^{*3}$ then $t' \equiv 1 \pmod{3}$ and hence the polynomial $3^{-3}\mathbf{g}(3x - \frac{t}{3}; t)$ has coefficients in $\mathfrak{O}_{F_{\mathfrak{p}}}$ and discriminant not divisible by \mathfrak{p} . Therefore \mathfrak{p} is unramified in K . If $\delta(\mathbf{g}) \in F_{\mathfrak{p}}^{*3}$ then $t' \not\equiv 1 \pmod{3}$ and hence the polynomial $\frac{3^3x^3}{(2t+3)\delta(\mathbf{g})}\mathbf{g}(\frac{3}{x} - \frac{t}{3}; t)$ turns out to be an Eisenstein polynomial for \mathfrak{p} . Thus \mathfrak{p} ramifies in K . It is a fact that $n_{\mathfrak{p}} \leq 2$ for any \mathfrak{p} when 3 is unramified in F . Therefore $n_{\mathfrak{p}}$ is equal to either 1 or 2 according to \mathfrak{p} ramifies tamely or wildly, respectively. \square

The following is immediate from the above proposition.

Corollary 8.2. *Assume 3 splits completely in F and $\delta(\mathbf{g}) \notin F_{\mathfrak{p}}^{*3}$ for each $\mathfrak{p} \mid 3$. Then a finite prime \mathfrak{p} of F ramifies in K if and only if $3 \nmid \nu_{\mathfrak{p}}(\delta(\mathbf{g})) > 0$.*

Acknowledgements

I would like to thank Professor Masanobu Kaneko for helpful suggestions and supports.

References

- [1] N. Aoki, Selmer Groups and Ideal Class Groups, *Comment. Math. Univ. St. Pauli* **42** (1993), no. 2, 209–229.
- [2] A. Brumer and K. Kramer, The rank of elliptic curves, *Duke Math. J.* **44** (1977), 715–743.
- [3] J. W. S. Cassels, Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer, *J. Reine Angew. Math.* **217** (1965), 180–199.
- [4] J. W. S. Cassels, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* **41** (1966), 193–291.
- [5] J. W. S. Cassels, *Lectures on Elliptic Curves*, London Math. Soc. Stud. Texts **24** (1991), Cambridge Univ. Press.
- [6] M. N. Gras, Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de \mathbb{Q} , *J. Reine Angew. Math.* **277** (1975), 89–116.
- [7] H. Hasse, Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol, *Nachr. Ges. Wiss. Göttingen, Math. Phys. Kl.* (1931), 64–69.
- [8] D. Husemöller, *Elliptic Curves*, Grad. Texts in Math. **111** (1987), Springer-Verlag.
- [9] R. Kozuma, A note on elliptic curves with a rational 3-torsion, preprint.
- [10] E. F. Schaefer, Class groups and Selmer groups, *J. Number Theory* **56** (1996), 79–114.
- [11] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. **106** (1986), Springer-Verlag.
- [12] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. **151** (1994), Springer-Verlag.
- [13] J. Top, Descent by 3-isogeny and 3-rank of quadratic fields, *Adv. in Number Theory* (1993), 303–317, Oxford Univ. Press.
- [14] L. C. Washington, Class Numbers of the Simplest Cubic Fields, *Math. Comp.* **48** (1987), 371–384.

GRADUATE SCHOOL OF MATHEMATICS, KYUSHU UNIVERSITY, FUKUOKA 812-8581, JAPAN

E-mail address: rinrin@math.kyushu-u.ac.jp